International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The GDPR and India's Data Protection Regime: Comparative Lessons, Constitutional Challenges

Mr.Gunnam Bhaskar Rao[1], Dr. Malay Kumar Behera[2], Prof. (Dr.) Sudhansu Ranjan Mohapatra[3]

[1]Phd Scholar, P G Dept Of Law, Sambalpur University
[2]Lecturship-Former, Law, Birla Global University
[3]Professor & Head, Dept Of Law, Guru Ghasidas University

Abstract

The emergence of data-driven governance has transformed personal information into a source of economic, administrative and political power. Contemporary privacy harms no longer arise solely from unauthorised disclosure or physical intrusion; they increasingly result from the continuous collection, aggregation, profiling, inference and automated use of personal data by both public and private actors. The European Union's General Data Protection Regulation (GDPR) represents the most influential contemporary model of comprehensive data protection. It combines principles governing data processing, multiple lawful bases, enforceable data-subject rights, organisational accountability, independent supervision and safeguards relating to automated decision-making. India has developed along a different constitutional trajectory. The recognition of privacy as a fundamental right in *Justice K S Puttaswamy (Retd) v Union of India* supplied a constitutional foundation for informational privacy grounded in dignity, autonomy, liberty and proportionality. The Digital Personal Data Protection Act 2023 (DPDP Act) and the Digital Personal Data Protection Rules 2025 constitute India's principal attempt to establish a dedicated statutory framework for digital personal data.

This article argues that the central comparative question is not whether India should replicate the GDPR. Such an inquiry assumes that regulatory similarity is the appropriate measure of legal adequacy. This article advances instead a **constitutional equivalence model of comparative data protection**. Under this model, a domestic data protection regime need not reproduce the institutional or textual architecture of the GDPR, but it must provide functionally equivalent safeguards against arbitrary and disproportionate concentrations of informational power. The constitutional adequacy of India's regime should therefore be measured by its capacity to protect dignity, autonomy, equality and democratic participation while subjecting both State and corporate data processing to meaningful legality, necessity, proportionality, accountability and oversight.

The article undertakes a detailed section-by-section comparison of the GDPR and the DPDP Act in relation to scope, processing principles, consent, lawful grounds, individual rights, sensitive data, children's data, accountability, automated decision-making, regulatory institutions, State exemptions, penalties and cross-border transfers. It argues that India has deliberately adopted a simplified and distinctive framework rather than a GDPR clone. However, certain differences are not merely matters of legislative style. The limited treatment of profiling and consequential automated decision-making, the

breadth of certain State exemptions, questions concerning institutional independence and the limited statutory articulation of data minimisation and purpose limitation raise constitutional concerns.
The article concludes that India should pursue neither wholesale transplantation nor regulatory exceptionalism. Instead, it should develop an indigenous model of constitutional data governance based on constitutional equivalence, differentiated accountability, independent oversight, algorithmic safeguards and proportionate regulation of informational power.

Keywords: GDPR; Digital Personal Data Protection Act 2023; DPDP Rules 2025; privacy; *Puttaswamy*; constitutionalism; comparative law; data protection; algorithmic accountability; digital governance.

I. INTRODUCTION

The contemporary digital economy is increasingly organised around the collection and use of personal information. Governments rely upon digital databases for welfare delivery, identity verification, taxation, policing, health administration and public services. Private corporations process personal data to provide communication services, financial products, digital platforms, targeted advertising and increasingly artificial intelligence-enabled services. The growth of data-intensive technologies has produced substantial economic and social benefits. Yet it has also fundamentally altered the distribution of power between individuals and institutions.

The principal difficulty is no longer adequately described by the traditional language of secrecy. An individual may reveal no sensitive information publicly and nevertheless become the subject of extensive profiling. Information supplied for one purpose may be combined with information obtained elsewhere. Seemingly innocuous data may generate highly sensitive inferences about health, financial status, political preferences or behavioural tendencies. Decisions affecting employment, credit, welfare or access to services may increasingly be shaped by computational systems whose operations are neither visible nor intelligible to the individuals affected.

Privacy consequently has acquired a broader constitutional significance. It concerns the conditions under which individuals remain capable of exercising autonomy in an environment characterised by pervasive informational asymmetry. It also concerns the constitutional limitation of institutional power. The ability to collect, classify and predict human behaviour can alter the relationship between the citizen and the State and between consumers and dominant technology platforms.

The European Union's General Data Protection Regulation has become the most influential legal response to this transformation.[1] Its significance lies not simply in the breadth of its territorial reach or the severity of its penalties. The GDPR represents a particular regulatory philosophy. Personal data processing is treated as an activity requiring continuing legal justification. Controllers are subject to substantive principles. Individuals possess enforceable rights. Organisations must demonstrate accountability. Supervisory authorities perform institutional oversight. Certain forms of solely automated decision-making are expressly regulated.

India's legal development has followed a different path. Prior to the recognition of privacy as a fundamental right, protection of personal information was fragmented across constitutional principles,

[1] 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 [2016] OJ L119/1 (GDPR).

the Information Technology Act 2000, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 and sector-specific regulation.[2] The inadequacy of this framework became increasingly apparent as data processing moved beyond conventional computer security and electronic commerce.

The constitutional landscape was transformed by the Supreme Court's nine-judge Bench decision in *Justice K S Puttaswamy (Retd) v Union of India*.[3] The Court recognised privacy as a fundamental right and linked it with liberty, dignity, autonomy and personhood. The judgment also established that intrusions upon privacy must satisfy constitutional requirements of legality, legitimate purpose, proportionality and procedural safeguards.[4]

The Digital Personal Data Protection Act 2023 represents an important legislative response to this constitutional development. The Act seeks to regulate the processing of digital personal data while recognising both the individual's interest in protecting personal data and the need to process such data for lawful purposes.[5] The Digital Personal Data Protection Rules 2025 provide further operational detail. However, India's regime is being brought into operation in phases. Consequently, as of 26 August 2026, the enacted framework and the fully operative substantive regime must be analytically distinguished. The official commencement notification schedules the principal processing provisions for later commencement, while the Rules themselves prescribe staggered timelines.

This temporal position is important. It would be premature to evaluate the Indian regime solely through its mature enforcement outcomes. Nevertheless, the statutory architecture itself can and should be subjected to constitutional and comparative scrutiny.

The central question of this article is therefore not whether India should adopt the GDPR. That question is both conceptually and normatively inadequate. Legal systems may pursue comparable constitutional objectives through different institutional arrangements.

This article instead asks:

Can India's data protection regime provide constitutionally equivalent protection against informational power without reproducing the GDPR's institutional and textual architecture?

The article advances the following central proposition:

Comparative adequacy in data protection should be measured by constitutional equivalence rather than regulatory similarity. India need not transplant the GDPR, but it must develop safeguards functionally capable of constraining disproportionate informational power and protecting the constitutional values recognised in Puttaswamy.

This proposition has three implications.

First, differences between the GDPR and the DPDP Act should not automatically be treated as deficiencies. India may legitimately develop different concepts, procedures and institutions.

Secondly, certain differences may nevertheless reveal a constitutional deficit. Where an alternative model fails to provide a functionally comparable safeguard against significant risks to autonomy, equality or democratic freedom, regulatory difference cannot be defended merely as domestic policy choice.

[2] Information Technology Act 2000; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
[3] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[4] ibid.
[5] Digital Personal Data Protection Act 2023, long title.

Thirdly, the Indian Constitution should operate as the normative filter for comparative borrowing. Comparative law may provide institutional lessons, but the ultimate constitutional standard must be derived from India's own constitutional order.

The uploaded doctoral research provides the broader foundation for this approach. It argues that privacy should be understood as a structural constitutional value and that comparative privacy governance is useful only when principles are adapted to India's constitutional and institutional context.

II. RESEARCH PROBLEM, OBJECTIVES AND METHODOLOGY

A. Research Problem

Much of the contemporary discussion of India's data protection law proceeds by asking whether the DPDP Act is stronger or weaker than the GDPR. Such comparisons are useful but incomplete. They frequently assume that the European model represents a universal regulatory benchmark and that legal divergence is evidence of regulatory inadequacy.

This article rejects that assumption.

The problem is instead whether the Indian legal framework provides constitutionally sufficient constraints upon the exercise of informational power. This requires analysis of both State and private actors and of contemporary forms of data processing that extend beyond collection and disclosure to inference, profiling and automated decision-making.

B. Objectives

The article has five principal objectives:

1. to examine the normative architecture of the GDPR;
2. to analyse the constitutional foundations of India's data protection regime;
3. to undertake a detailed section-by-section comparison of the GDPR and the DPDP Act;
4. to identify the limits of mechanical legal transplantation; and
5. to develop the constitutional equivalence model as a framework for future Indian data governance.

C. Research Questions

The article addresses the following questions:

1. What constitutional and regulatory philosophy underlies the GDPR?
2. How has *Puttaswamy* shaped the constitutional basis of data protection in India?
3. In what respects does the DPDP Act converge with and depart from the GDPR?
4. Which differences represent legitimate contextual adaptation, and which may create constitutional vulnerabilities?
5. Can India develop functionally equivalent safeguards without reproducing the European model?

D. Methodology

The study employs doctrinal and comparative legal methodology. The doctrinal analysis examines constitutional jurisprudence, the GDPR, the DPDP Act and the DPDP Rules. The comparative analysis does not proceed merely by juxtaposing statutory provisions. It evaluates whether legal mechanisms perform comparable constitutional functions.

This distinction is important. A comparative study based solely upon textual similarity may conclude that a domestic statute is deficient because it does not contain a particular foreign provision. A functional constitutional comparison asks a different question: **what risk does the foreign provision address, and does the domestic system provide another effective mechanism addressing the same risk?**

This article therefore adopts a three-stage methodology:

Stage One: Identification of Risk

What form of informational power or privacy harm is being regulated?

Stage Two: Identification of Safeguard

What substantive, procedural or institutional mechanism constrains that risk?

Stage Three: Constitutional Equivalence

Does the domestic mechanism provide functionally sufficient protection of the constitutional interests at stake?

This methodology forms the original analytical framework of the article.

III. THE GDPR: REGULATING PERSONAL DATA THROUGH STRUCTURAL ACCOUNTABILITY

A. Data Protection as a Regulatory System

The GDPR is frequently described as a comprehensive data protection law. That description is correct but insufficient. Its distinctive feature is the integration of individual rights with institutional and organisational obligations.

The Regulation does not assume that privacy can be protected exclusively through individual consent. Nor does it assume that harm can be adequately remedied through litigation after it occurs. Instead, it establishes a system of continuing governance.

The GDPR regulates:

- the principles governing processing;
- the conditions of lawful processing;
- the processing of special categories of data;
- transparency obligations;
- individual rights;
- controller and processor responsibilities;
- security;
- breach notification;
- impact assessments;
- data protection by design and by default;
- international transfers; and
- supervisory and enforcement mechanisms.

This architecture reflects the recognition that data protection is a systemic problem.

B. Article 5: Principles of Processing

Article 5 is central to the GDPR's architecture. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; limited to what is necessary; accurate; retained only as long as necessary; and processed with appropriate security. The controller is also responsible for demonstrating compliance.[6]

These principles are significant because they restrain data processing before an individual right is invoked.

[6] GDPR art 5.

Data minimisation, for example, asks whether the information should have been collected at all. Purpose limitation asks whether information collected for one objective may legitimately be deployed for another. Storage limitation constrains the indefinite retention of data.

The accountability principle adds a structural dimension. The organisation must not merely claim compliance after a dispute; it must be capable of demonstrating it.

C. Article 6: Lawful Bases

The GDPR recognises several lawful bases for processing. Consent is only one of them. Processing may also be lawful where necessary for contractual performance, legal obligations, vital interests, public tasks or legitimate interests, subject to applicable conditions.[7]

This approach reflects an important regulatory insight: consent cannot bear the entire burden of data governance. Modern society requires numerous forms of processing that do not depend upon individual negotiation. However, the existence of alternative lawful grounds does not eliminate the application of Article 5 principles.

D. Individual Rights

The GDPR provides a broad catalogue of data-subject rights, including rights to information, access, rectification, erasure, restriction, portability and objection.[8]

The right to portability is particularly relevant to the relationship between data protection and market power. The right to object may constrain certain forms of processing even where the controller relies upon lawful grounds other than consent.

These rights do not simply create remedies. They redistribute informational agency.

E. Automated Decision-Making and Profiling

Article 22 provides that, subject to specified exceptions, an individual has the right not to be subject to a decision based solely on automated processing, including profiling, where the decision produces legal or similarly significant effects. Where certain exceptions apply, safeguards include human intervention, the opportunity to express a point of view and the ability to contest the decision.[9]

The provision is particularly important because data protection increasingly concerns decisions derived from data rather than the possession of data itself.

The GDPR's official text expressly identifies Article 22 as a safeguard against solely automated decisions producing legal or similarly significant effects.

F. Accountability and Privacy by Design

Articles 24 and 25 impose responsibilities upon controllers to implement appropriate measures and to integrate data protection into systems and processes.[10]

The preventive orientation of these provisions is particularly relevant in complex technological systems. Once a large-scale surveillance or algorithmic infrastructure is operational, individual remedies may be ineffective. Privacy must therefore be considered during design rather than only after deployment.

G. Independent Supervision

The GDPR requires independent supervisory authorities.[11] Their independence is institutionally significant because data controllers may include powerful public and private organisations.

[7] GDPR art 6.
[8] GDPR arts 12–21.
[9] GDPR art 22.
[10] GDPR arts 24–25.
[11] GDPR arts 51–59.

The European model therefore demonstrates that effective data protection requires more than substantive rights. It requires institutions capable of enforcing those rights.

H. Limits of the GDPR Model

The GDPR should not be treated as a perfect model. It has been criticised for complexity, compliance burdens and difficulties in achieving consistent enforcement.[12] The practical regulation of global technology corporations also remains challenging.

The comparative lesson for India is therefore not that more detailed legislation necessarily produces better protection. The more important lesson is that **rights require an institutional ecosystem capable of converting legal principles into practical constraints upon power**.

IV. INDIA'S CONSTITUTIONAL PATH TO DATA PROTECTION

A. Privacy before Puttaswamy

Indian privacy jurisprudence developed incrementally through constitutional interpretation. Early cases reflected uncertainty about whether privacy constituted an independent fundamental right. The expansion of Article 21 gradually supplied a broader constitutional foundation for personal liberty.

The development of constitutional privacy must be understood within the broader transformation of Indian constitutional law following *Maneka Gandhi v Union of India*.[13] Article 21 ceased to be understood narrowly as a purely procedural guarantee. The relationship between liberty, reasonableness and constitutional fairness became more substantive.

B. Puttaswamy and the Transformation of Privacy

Justice K S Puttaswamy (Retd) v Union of India marked the decisive constitutional turning point. The Supreme Court held that privacy is a constitutionally protected fundamental right arising primarily from Articles 14, 19 and 21.[14]

The importance of the decision lies in at least four propositions.

1. Privacy is linked with dignity

Privacy protects the conditions under which individuals develop and express their personality.

2. Privacy is linked with autonomy

The constitutional significance of privacy extends to decisional and informational autonomy.

3. Informational privacy is constitutionally relevant

The judgment recognised that technological developments require constitutional protection against the misuse of personal information.

4. Privacy is not absolute

Restrictions must satisfy constitutional standards of legality, legitimate State interest, proportionality and procedural safeguards.

These principles make *Puttaswamy* particularly significant for data protection legislation.

C. From Individual Privacy to Informational Power

The constitutional challenge of digital governance cannot be reduced to whether an individual has consented to a particular transaction.

[12] Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179.
[13] Maneka Gandhi v Union of India (1978) 1 SCC 248.
[14] Puttaswamy (n 3).

Consider a platform that lawfully collects information through consent. It may subsequently combine that information with behavioural data, location patterns and inferences generated through machine learning. The individual may never have directly disclosed the final profile.

The constitutional question therefore becomes one of informational power.

The thesis underlying this article similarly argues that contemporary privacy harms arise from aggregation, predictive profiling and automated decision-making and that privacy must operate as a limitation on excessive informational power.

This insight requires Indian data protection law to be evaluated not only as a consumer-protection mechanism but as an element of constitutional governance.

V. THE DPDP ACT 2023: STRUCTURE, PURPOSE AND REGULATORY PHILOSOPHY

A. Legislative Purpose

The long title of the DPDP Act states that it regulates the processing of digital personal data in a manner recognising both the individual's right to protect personal data and the need to process such data for lawful purposes.[15]

This formulation is significant. The Act does not present data protection as an absolute prohibition upon processing. It expressly seeks to balance protection with lawful processing.

This orientation reflects India's broader digital policy environment, which includes economic development, innovation, digital public infrastructure and administrative efficiency.

B. Scope

Section 3 applies the Act to digital personal data processed within India where the data is collected digitally or collected in non-digital form and subsequently digitised. It also applies to certain processing outside India connected with the offering of goods or services to Data Principals within India.[16]

The digital focus distinguishes the DPDP Act from the GDPR's broader regulation of personal data processing generally.

This difference is not automatically constitutionally problematic. The more important question is whether significant categories of privacy harm are left outside effective protection.

C. Core Actors

The DPDP Act adopts its own terminology:

- **Data Principal**;
- **Data Fiduciary**; and
- **Data Processor**.

The Data Fiduciary is particularly important because it determines the purpose and means of processing.

The terminology of fiduciary responsibility potentially provides a useful conceptual basis for Indian law. A data fiduciary model can emphasise obligations arising from informational power rather than merely contractual relationships.

D. Consent

Section 6 establishes consent as a central basis for processing. Consent must be free, specific, informed, unconditional and unambiguous, with a clear affirmative action.[17]

Section 5 requires notice containing specified information.

[15] Digital Personal Data Protection Act 2023, long title.
[16] Digital Personal Data Protection Act 2023, s 3.
[17] ibid s 6 .

These requirements represent an effort to improve the quality of consent. However, the constitutional problem of consent is structural.

A formally valid consent may not necessarily reflect meaningful autonomy where:

- the service is indispensable;
- the individual has no realistic alternative;
- the processing is technically incomprehensible;
- the consequences arise from future inference;
- the interface is designed to manipulate decisions; or
- the user experiences repeated consent fatigue.

The thesis identifies these limitations and warns that consent may become formalistic in highly asymmetric digital environments.

The appropriate lesson is not to reject consent. It is to recognise that **consent is one safeguard among several and cannot substitute for structural limitations upon disproportionate processing**.

E. Legitimate Uses

Section 7 permits specified legitimate uses of personal data without consent.[18] These uses include circumstances relating to voluntary provision of data, performance of legal obligations, compliance with judgments and orders, medical emergencies, disasters and certain employment purposes, among others.

The provision illustrates a fundamental difference between the GDPR and DPDP models. The GDPR employs a general taxonomy of lawful bases. The DPDP Act operates through consent and legislatively specified legitimate uses.

Both approaches seek to address the same practical problem: data processing cannot always depend upon consent.

The constitutional question is whether the exceptions remain sufficiently defined and subject to accountability.

F. Obligations of Data Fiduciaries

The Act imposes obligations relating to:

- responsibility for compliance;
- accuracy and completeness in specified circumstances;
- reasonable security safeguards;
- notification of personal data breaches; and
- erasure where consent is withdrawn or the specified purpose is no longer served, subject to applicable legal requirements.[19]

These provisions represent an important move away from a purely rights-based framework towards organisational responsibility.

G. Significant Data Fiduciaries

Section 10 permits the Central Government to notify certain Data Fiduciaries as Significant Data Fiduciaries, having regard to factors such as volume and sensitivity of personal data, risks to the rights of Data Principals, potential impact upon sovereignty and integrity and other relevant considerations.[20]

This risk-based approach is potentially valuable for India. A small enterprise and a national-scale platform need not necessarily be regulated identically.

[18] ibid s 7.
[19] ibid ss 8–9.
[20] ibid s 10.

However, differentiated regulation must not become under-regulation. The designation process should be transparent and based upon clearly articulated risk criteria.

H. Rights of Data Principals

The Act provides rights relating to:

- access to information;
- correction, completion, updating and erasure;
- grievance redressal; and
- nomination.[21][21]

These rights are important but narrower in several respects than the GDPR's rights architecture.

The most significant comparative question concerns rights relating to portability, objection, profiling and automated decision-making.

VI. SECTION-BY-SECTION COMPARISON OF THE GDPR AND THE DPDP ACT

A. Comparative Matrix

Regulatory Issue	GDPR	DPDP Act 2023	Constitutional Assessment
Scope	Broad processing of personal data	Digital personal data	Digital focus may be legitimate, but protection must not leave serious privacy harms unregulated
Core principles	Art 5 expressly provides lawfulness, fairness, transparency, purpose limitation, minimisation, accuracy, storage limitation, security and accountability	Obligations dispersed across provisions	India could strengthen explicit structural principles
Lawful grounds	Art 6 provides multiple lawful bases	Consent and specified legitimate uses	Different drafting model, but both must prevent arbitrary processing
Consent	One lawful basis, subject to strict requirements	Central basis under s 6	Consent cannot carry the entire burden of constitutional protection
Purpose limitation	Express and central	Linked to specified purpose architecture	Stronger explicit controls on secondary use would improve equivalence
Data minimisation	Explicit Art 5 principle	No directly equivalent general formulation	Potential constitutional gap where large-scale collection is involved
Special categories	Art 9 provides enhanced protection	No equivalent general statutory category	Risk-sensitive differentiation may be desirable

[21] ibid ss 11–14.

Regulatory Issue	GDPR	DPDP Act 2023	Constitutional Assessment
Access	Arts 12–15	s 11	Functional convergence
Rectification	Art 16	s 12	Functional convergence
Erasure	Art 17	s 12	Partial convergence
Restriction of processing	Art 18	No equivalent general right	Potential gap
Data portability	Art 20	No equivalent right	Requires consideration, particularly for platform power
Objection	Art 21	No equivalent general right	Potential gap in relation to profiling and direct marketing
Automated decisions	Art 22	No equivalent comprehensive right	Major emerging constitutional concern
Accountability	Arts 5(2), 24	Data Fiduciary obligations	Convergence, though Indian framework is less elaborately structured
Privacy by design	Art 25	No equivalent general statutory formulation	Significant preventive safeguard worth adapting
Impact assessments	Art 35	Risk assessment obligations for SDFs through Act/Rules framework	Scope and implementation remain critical
Independent supervision	Independent supervisory authorities	Data Protection Board of India	Institutional independence and capacity require close scrutiny
State exemptions	Restrictions subject to EU legal framework and fundamental rights standards	Statutory exemptions and State powers	Constitutional proportionality remains essential
Cross-border transfers	Chapter V safeguards	s 16 and executive restrictions	Greater clarity and safeguards may be required
Penalties	Art 83	Schedule to DPDP Act	Enforcement effectiveness is institutionally dependent

The table demonstrates the central argument of this article. Similarity and adequacy are not synonymous. Some differences are legitimate adaptations. Others raise questions of constitutional equivalence.

B. Scope: GDPR Article 2 and DPDP Act Section 3

The GDPR generally applies to the processing of personal data wholly or partly by automated means and

to certain non-automated processing forming part of a filing system.[22]

The DPDP Act focuses upon digital personal data.

The GDPR therefore begins from a technologically neutral conception of personal data, whereas the DPDP Act is explicitly focused on digital processing.

This difference may reflect legislative practicality. India's principal contemporary privacy risks increasingly arise within digital environments. However, the exclusion of non-digital information systems should not be assumed to be constitutionally irrelevant.

The constitutional test should be functional. If a non-digital information system produces a serious invasion of informational autonomy, the absence of protection under the DPDP Act may require the application of other legal or constitutional safeguards.

C. Principles: GDPR Article 5 and the Indian Distributed Model

Article 5 of the GDPR is perhaps the clearest example of a structural regulatory philosophy. It establishes express principles applicable across processing.

The DPDP Act contains analogous concerns but does not reproduce the GDPR's Article 5 catalogue as a single provision.

This drafting difference matters.

An explicit principles provision can perform at least three functions:

1. **interpretive function** – guiding the interpretation of specific provisions;
2. **regulatory function** – providing standards for supervisory action; and
3. **constitutional function** – identifying the fundamental limitations upon informational power.

The absence of a single provision does not necessarily eliminate these protections. However, India would benefit from a clearer articulation of general principles of fairness, purpose discipline, minimisation and accountability.

The GDPR's official text identifies these principles as including purpose limitation and data minimisation.

For India, data minimisation is especially important because the constitutional doctrine of proportionality requires an inquiry into necessity. A State or corporation should not collect information merely because technological capacity makes collection convenient.

D. Consent: GDPR Articles 4, 6 and 7 and DPDP Act Sections 5 and 6

Both systems seek meaningful consent, but their structures differ.

Under the GDPR, consent is one lawful basis among several. Under the DPDP Act, consent is a central organising principle, supplemented by legitimate uses.

The advantage of India's model is conceptual simplicity. The disadvantage is the risk of overestimating the autonomy represented by consent.

A constitutionally adequate consent framework should ask not only whether consent was formally obtained but whether the individual had meaningful agency.

The following proposition should therefore guide Indian interpretation:

Where informational asymmetry, technological opacity or institutional dependence substantially undermine meaningful choice, formal consent should not immunise disproportionate data processing from constitutional scrutiny.

This is particularly relevant to public services and dominant platforms.

[22] GDPR art 2.

E. Sensitive Data: GDPR Article 9 and the DPDP Act

Article 9 of the GDPR establishes special protection for categories such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data and information concerning sex life or sexual orientation.[23]

The DPDP Act does not reproduce a general statutory distinction between ordinary and sensitive personal data.

This difference should not automatically be treated as fatal. A risk-based regime may protect sensitive information through the designation of Significant Data Fiduciaries, security obligations or sector-specific regulation.

Nevertheless, the absence of differentiated statutory protection raises a constitutional question.

Not all personal data carries equivalent risks. A breach involving a shopping preference does not ordinarily create the same risk as a breach involving biometric information, genetic information or highly sensitive health data.

The constitutional equivalence model therefore suggests that India need not copy Article 9. It should, however, develop **functionally equivalent enhanced safeguards for high-risk categories of information**.

F. Rights of Individuals

1. Access

GDPR Articles 12–15 and DPDP Act section 11 both recognise access-related rights.

This is a substantial area of convergence.

2. Rectification and Erasure

GDPR Articles 16 and 17 provide rectification and erasure rights. Section 12 of the DPDP Act similarly addresses correction, completion, updating and erasure.

However, the legal context and exceptions differ.

3. Restriction

GDPR Article 18 provides a right to restriction of processing in specified circumstances.

The DPDP Act does not provide a directly comparable general right.

A constitutional equivalence analysis asks whether other remedies sufficiently protect an individual during disputes about accuracy, legality or purpose. If disputed data continues to be processed while a grievance remains unresolved, correction after the event may be inadequate.

4. Portability

GDPR Article 20 creates a right to data portability in specified circumstances.

The DPDP Act contains no general equivalent.

Portability is not merely a privacy issue. It may reduce dependency upon dominant platforms and improve user agency.

India need not necessarily adopt the GDPR's exact provision. However, the absence of portability should be reconsidered in sectors characterised by significant data concentration or switching costs.

5. Objection

Article 21 provides a right to object in specified circumstances.

The absence of a broad comparable right in the DPDP Act is particularly relevant to profiling and certain forms of behavioural processing.

[23] GDPR art 9.

VII. AUTOMATED DECISION-MAKING: THE MOST SIGNIFICANT COMPARATIVE DIVIDE

The most important divergence between the GDPR and India's current statutory architecture concerns automated decision-making and profiling.

The GDPR does not completely prohibit automated decisions. Article 22 adopts a conditional framework. It identifies a category of decisions that produce legal or similarly significant effects and provides safeguards.

The Indian framework does not contain an equivalent comprehensive statutory provision.

This gap becomes increasingly significant as automated systems influence:

- recruitment;
- lending;
- insurance;
- welfare;
- education;
- healthcare;
- law enforcement;
- consumer pricing; and
- access to digital services.

The constitutional issue is broader than privacy.

An algorithm may generate discrimination without disclosing personal information. A system may rely upon inaccurate inferences. An affected person may be unable to understand why an adverse decision was reached.

The thesis's analysis similarly identifies algorithmic profiling and automated decision-making as areas insufficiently addressed by existing Indian privacy regulation.

India should therefore enact a dedicated framework for **consequential automated decision-making**. Such a framework should apply where automated processing materially affects rights, opportunities or access to significant services.

The proposed safeguards should include:

1. prior risk assessment;
2. notice that consequential automation is being used;
3. meaningful information about the relevant basis of the decision;
4. human review where appropriate;
5. a right to challenge significant decisions;
6. testing for discriminatory outcomes; and
7. independent audit of high-risk systems.

This proposal does not require transplantation of Article 22. It seeks constitutional equivalence.

VIII. ACCOUNTABILITY, PRIVACY BY DESIGN AND PREVENTIVE GOVERNANCE

A central lesson of the GDPR is that data protection should not depend exclusively upon individual enforcement.

Article 25 requires data protection by design and by default.[24] Article 35 requires data protection impact assessments in certain high-risk circumstances.[25]

These provisions are preventive.

India's Data Fiduciary model can potentially develop an equally significant accountability culture. The fiduciary terminology itself can be used to impose heightened responsibilities upon entities exercising substantial informational power.

The proposed Indian model should distinguish between ordinary and high-risk processing.

Ordinary processing

Entities should comply with baseline obligations relating to notice, security, accuracy and purpose.

High-risk processing

Enhanced requirements should apply where processing involves:

- large populations;
- sensitive information;
- children;
- biometric identification;
- systematic surveillance;
- behavioural profiling;
- consequential automated decisions; or
- substantial risk of discrimination.

High-risk Data Fiduciaries should be subject to:

- privacy impact assessments;
- algorithmic impact assessments where applicable;
- independent audits;
- enhanced breach reporting;
- documented governance systems; and
- periodic review.

This approach would be more appropriate for India than indiscriminately imposing identical GDPR-style compliance obligations upon every organisation.

IX. THE DATA PROTECTION BOARD OF INDIA AND THE QUESTION OF INSTITUTIONAL INDEPENDENCE

The DPDP Act establishes the Data Protection Board of India. The Board is a central component of the enforcement architecture.

As a matter of current law, the institutional provisions were among those brought into force by the 13 November 2025 commencement notification. Official materials subsequently issued in 2026 indicate continuing steps regarding appointment of the Chairperson and members.

The constitutional issue is not simply whether a Board exists.

The critical question is whether the institution possesses sufficient:

- functional independence;
- expertise;
- technological competence;

[24] GDPR art 25.
[25] GDPR art 35.

- procedural autonomy;
- transparency;
- resources; and
- authority to scrutinise both private and public power.

This is especially important because the State is itself a major processor of personal information.

A data protection authority may be required to consider complaints involving public databases, governmental processing or powerful technology corporations. Its legitimacy therefore depends upon the public perception and institutional reality of independence.

The GDPR offers an important lesson in this regard. Independent supervision is not merely an administrative preference. It is a structural safeguard against concentration of informational power.

The thesis likewise identifies institutional independence as one of the most important comparative lessons for India.

The constitutional equivalence model therefore requires the following question:

Does the Indian institutional arrangement provide an effective and sufficiently independent mechanism for supervising entities whose processing power may affect fundamental rights?

If the answer is negative, the existence of a formally established Board cannot itself establish constitutional adequacy.

X. STATE EXEMPTIONS, SURVEILLANCE AND CONSTITUTIONAL PROPORTIONALITY

The most difficult question in Indian data protection law concerns the State.

Private corporations are important processors of personal information, but governmental data processing implicates additional constitutional concerns because the State possesses coercive authority.

Public authorities may collect data in connection with:

- taxation;
- welfare;
- identity systems;
- law enforcement;
- national security;
- immigration;
- public health; and
- regulatory administration.

Such processing may be legitimate and necessary. Constitutionalism does not require the State to abandon digital governance.

However, *Puttaswamy* establishes that interference with privacy cannot be justified merely by invoking administrative convenience.

The constitutional inquiry requires:

1. **Legality** – Is there a clear legal basis?
2. **Legitimate aim** – Is the objective constitutionally legitimate?
3. **Necessity** – Is the processing genuinely necessary?
4. **Proportionality** – Is the measure appropriately tailored?
5. **Procedural safeguards** – Is there meaningful oversight and a remedy against abuse?

The thesis argues that comparative data protection models demonstrate the importance of surveillance safeguards and meaningful institutional or judicial review.

The critical proposition is that statutory exemptions cannot be treated as constitutionally self-validating. A statute may authorise an exemption, but its application remains subject to constitutional scrutiny where fundamental rights are affected.

India should therefore develop enhanced safeguards for high-risk State processing, including:

- defined statutory purposes;
- retention limits;
- necessity assessments;
- independent oversight;
- periodic review;
- transparency reporting where possible; and
- effective remedies.

For particularly intrusive surveillance, judicial or independently authorised oversight should be seriously considered.

XI. CROSS-BORDER DATA TRANSFERS: FROM DATA SOVEREIGNTY TO CONSTITUTIONAL SAFEGUARDS

Cross-border data flows complicate conventional territorial regulation.

The GDPR adopts a detailed framework for transfers to third countries and international organisations.[26] It employs mechanisms including adequacy decisions and specified safeguards.

The DPDP Act adopts a different approach under section 16, permitting the Central Government to restrict transfers to notified countries or territories.[27]

The two systems reflect different regulatory philosophies.

The GDPR begins with the concern that personal data should not lose legal protection merely because it crosses a border.

The Indian model provides greater executive flexibility.

Neither absolute data localisation nor unrestricted data flows should be treated as constitutionally inevitable.

A constitutionally appropriate Indian model should consider:

- the nature and sensitivity of data;
- the purpose of transfer;
- risks of foreign surveillance;
- enforceability of individual rights;
- the availability of effective remedies;
- cybersecurity implications; and
- India's legitimate interests in digital trade and innovation.

The thesis identifies cross-border transfers as an area requiring clearer safeguards and accountability.

The constitutional equivalence model therefore supports a **risk-sensitive transfer framework** rather than an indiscriminate policy of either localisation or liberalisation.

XII. THE LIMITS OF LEGAL TRANSPLANTATION

Comparative law can be extremely valuable, but legal transplantation has limits.

[26] GDPR arts 44–50.
[27] Digital Personal Data Protection Act 2023, s 16.

The GDPR emerged within a particular constitutional and institutional environment. European data protection law operates within a legal order that includes supranational institutions, fundamental rights instruments and a long history of regulatory supervision.

India has a different constitutional structure and a different digital environment.

India must account for:

- demographic scale;
- linguistic diversity;
- digital literacy disparities;
- large-scale public digital infrastructure;
- extensive biometric identification;
- rapidly growing start-ups and digital enterprises;
- developmental priorities;
- federal governance structures; and
- the practical need for accessible regulatory institutions.

These differences justify contextual adaptation.

However, context must not become an argument for constitutional dilution.

A developing digital economy does not require weaker constitutional protection. It requires a regulatory architecture capable of achieving rights protection without imposing unnecessary or disproportionate compliance burdens.

This is why the distinction between **regulatory similarity** and **constitutional equivalence** is essential.

XIII. THE CONSTITUTIONAL EQUIVALENCE MODEL: A PROPOSED ORIGINAL FRAMEWORK

This article proposes a five-part constitutional equivalence model.

A. Functional Equivalence

The question is not whether India has copied a GDPR provision.

The question is whether the Indian system provides an alternative mechanism capable of addressing the same constitutional risk.

For example:

- Article 9 of the GDPR protects special categories of data.
- India need not reproduce Article 9.
- But high-risk data should receive functionally enhanced protection.

B. Proportionality Equivalence

The intensity of regulation should correspond to the intensity of risk.

A small business processing limited information should not necessarily bear the same obligations as a platform processing information relating to millions of individuals.

Conversely, high-risk processing should attract enhanced obligations.

C. Institutional Equivalence

Formal rights are ineffective without enforcement.

The institutional structure must be capable of investigating breaches, imposing consequences and scrutinising powerful actors.

D. Procedural Equivalence

Individuals affected by significant data processing should possess meaningful procedural opportunities.

This includes, where appropriate:

- notice;
- access;
- correction;
- explanation;
- contestation;
- human review; and
- an effective remedy.

E. Constitutional Equivalence

The ultimate standard is whether the system protects the constitutional interests recognised in *Puttaswamy*.

These include:

- dignity;
- autonomy;
- liberty;
- informational self-determination;
- equality;
- proportionality; and
- democratic participation.

This model avoids two unsatisfactory extremes.

The first is **legal transplantation**, under which the GDPR is treated as a universal statutory template.

The second is **regulatory exceptionalism**, under which domestic context is used to justify inadequate safeguards.

The constitutional equivalence model occupies the normative space between them.

XIV. PROPOSALS FOR AN INDIAN MODEL OF CONSTITUTIONAL DATA GOVERNANCE

A. Express Data Processing Principles

India should consider an express statutory articulation of:

- fairness;
- purpose limitation;
- necessity and minimisation;
- accuracy;
- storage discipline;
- security; and
- accountability.

These principles would provide interpretive coherence.

B. High-Risk Data Classification

Rather than mechanically importing the GDPR's sensitive-data categories, India should develop enhanced safeguards for high-risk information.

The classification should be responsive to the nature and consequences of processing.

C. Algorithmic Accountability Legislation

India should establish specific safeguards for consequential automated decisions.

This should include impact assessments, human review, contestation and anti-discrimination obligations.

D. Meaningful Consent Standards

Consent should be evaluated in light of actual informational and bargaining conditions.

The law should be especially vigilant where services are essential or alternatives are unrealistic.

E. Privacy by Design

High-risk technological systems should incorporate privacy safeguards during development rather than after deployment.

F. Strengthened Institutional Independence

The Data Protection Board should possess sufficient functional independence, technological expertise and procedural autonomy.

G. Proportionate State Processing

Governmental processing should remain subject to legality, necessity, proportionality and procedural safeguards.

H. Risk-Based Cross-Border Transfers

Transfer regulation should protect rights without unnecessarily restricting legitimate digital activity.

I. Integration with AI Governance

Data protection law and AI governance should not develop in complete isolation.

AI systems frequently create privacy, equality and due-process concerns simultaneously.

XV. FINDINGS

The article produces the following principal findings.

1. The GDPR remains a valuable comparative model but not a universal legislative template.

Its greatest contribution is the development of structural accountability.

2. Puttaswamy provides India with an independent constitutional foundation.

India need not import the constitutional justification for data protection from Europe.

3. The DPDP Act represents a significant transition in Indian law.

India has moved from fragmented protection towards a dedicated statutory framework.

4. Regulatory difference is not necessarily constitutional deficiency.

India may legitimately adopt distinctive concepts and institutions.

5. Certain differences require closer constitutional scrutiny.

These include:

- automated decision-making;
- profiling;
- high-risk data;
- State exemptions;
- regulatory independence; and
- structural accountability.

6. Consent is necessary but insufficient.

Meaningful privacy protection requires limits upon processing even where formal consent exists.

7. The greatest future challenge concerns data-derived power.

The central legal question is increasingly not who possesses data, but what can be inferred and decided through it.

8. India should pursue constitutional equivalence.

The objective should be functionally effective protection of constitutional rights rather than textual repli-

cation of foreign law.

XVI. CONCLUSION

The comparison between the GDPR and India's data protection regime should not be framed as a competition between a mature European model and an incomplete domestic alternative. Such a comparison risks obscuring the more important constitutional question.

The GDPR and the DPDP Act emerge from different legal traditions and regulatory environments. The GDPR is embedded in a rights-oriented European legal order characterised by detailed principles, supervisory authorities and an extensive institutional structure. India's DPDP Act operates within a constitutional framework transformed by *Puttaswamy* and within a rapidly expanding digital society marked by developmental priorities, large-scale public digital infrastructure and substantial technological diversity.

India is therefore neither required nor necessarily advised to reproduce the GDPR.

Yet constitutional context cannot justify an absence of effective protection.

The recognition of privacy as a fundamental right requires Indian law to address the realities of contemporary informational power. Data protection cannot be confined to notice, consent and post-breach remedies. It must also address excessive collection, secondary use, profiling, automated decision-making, institutional surveillance and the concentration of informational power.

The central contribution of this article is the proposition that comparative adequacy should be assessed through **constitutional equivalence rather than regulatory similarity**.

Under this approach, India may reject wholesale legal transplantation. It may develop its own terminology, institutions and compliance structures. It may employ differentiated regulation suited to the scale and diversity of its digital economy.

However, it must ensure that these alternatives provide functionally sufficient protection against the constitutional risks created by data-intensive technologies.

The Indian model should therefore be built upon five pillars:

1. **constitutional proportionality;**
2. **structural accountability;**
3. **independent institutional oversight;**
4. **procedural safeguards against consequential data-driven decisions; and**
5. **risk-sensitive regulation of informational power.**

The GDPR provides valuable lessons concerning each of these pillars. The task for India is not to copy them mechanically.

It is to constitutionalise them.

The future of Indian data protection should therefore not be defined by the question, **“How closely does India resemble Europe?”**

The more fundamental question is:

“Does India's legal system provide constitutionally effective safeguards against the forms of informational power that increasingly shape the freedom, equality and autonomy of individuals?”

That is the appropriate measure of success for India's evolving data protection regime.

BIBLIOGRAPHY

Cases

1. *Aadhaar (Justice K S Puttaswamy (Retd) v Union of India)* (2019) 1 SCC 1.
2. *Gobind v State of Madhya Pradesh* (1975) 2 SCC 148.
3. *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
4. *Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295.
5. *M P Sharma v Satish Chandra* AIR 1954 SC 300.
6. *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
7. *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.
8. *R Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632.
9. *Shreya Singhal v Union of India* (2015) 5 SCC 1.

Legislation

1. Constitution of India 1950.
2. Digital Personal Data Protection Act 2023.
3. Digital Personal Data Protection Rules 2025.
4. General Data Protection Regulation, Regulation (EU) 2016/679.
5. Information Technology Act 2000.
6. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

Reports and Official Materials

1. Committee of Experts under Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Government of India 2018).
2. Justice AP Shah Committee, *Report of the Group of Experts on Privacy* (Planning Commission 2012).

Books and Articles

1. Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008).
2. Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).
3. Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press 2014).
4. Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015).
5. Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).
6. Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.
7. Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 *Computer Law & Security Review* 179.