

Privacy Beyond the Phone Setting: Articles 14, 19 and 21 after Puttaswamy and the Constitutional Questions Raised by India's Data-Protection Framework

Yuvraj

Academic article | OSCOLA edition 5 | Publication version 1

Article citation: Yuvraj, "Privacy Beyond the Phone Setting: Articles 14, 19 and 21 after Puttaswamy and the Constitutional Questions Raised by India's Data-Protection Framework", The Legal Gazette — Open Scholarship (2026-10-22), version 1, <https://www.thelegalgazette.org/scholarship/803684b2-19a7-4825-8915-793e7b2ee5c8>.

Downloaded: 2026-10-22T19:27:18.352Z UTC | 23 Oct 2026, 00:57:18 IST

Abstract

The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v Union of India transformed Indian constitutional analysis. Privacy is not confined to secrecy or personal information: it protects bodily integrity, decisional autonomy, intimate life and the conditions in which other freedoms can be exercised. This article examines the contribution of Articles 21, 19 and 14 of the Constitution, and explains the legality, legitimate-aim, proportionality and safeguards framework through which State interference is assessed. It then considers the Digital Personal Data Protection Act, 2023 (DPDP Act), the Digital Personal Data Protection Rules, 2025, and the constitutional questions raised by exemptions for State and law-enforcement processing, government information demands, the amendment to the Right to Information Act, 2005, and the design of the Data Protection Board. The comparison with the European Union's General Data Protection Regulation is used as a contrast in regulatory design, not as a substitute for Indian constitutional analysis. As at 22 October 2026, public case trackers report that the constitutional challenge to parts of the Indian framework remains pending and that no challenged provision has been struck down or suspended. The central argument is that privacy does not decide every dispute by itself; it supplies a constitutional standard against which the legal basis, purpose, necessity, proportionality and safeguards of an interference must be examined.

Keywords: privacy, constitutional law, Article 14, Article 19, Article 21, Puttaswamy, proportionality, Digital Personal Data Protection Act 2023, right to information, GDPR

1. Introduction

Digital privacy is often discussed through the familiar devices of a password, a lock screen or a consent banner. Those devices may be useful, but they do not define the legal right. In India, privacy has constitutional significance because it protects the individual's dignity, autonomy and ability to make choices without unjustified intrusion. The Supreme Court's nine-judge decision in Justice K.S. Puttaswamy (Retd.) v Union of India settled that the right to privacy is protected by Part III of the Constitution, principally through Article 21 and in conjunction with the other fundamental freedoms.[1]

The doctrine did not appear fully formed in 2017. Earlier decisions reached different conclusions about the relationship between privacy, search and seizure, police surveillance and personal liberty. Later decisions protected privacy in particular contexts, while the exact constitutional position remained unsettled at the level of a binding nine-judge ruling. Puttaswamy resolved that central question, but it did not make privacy

absolute or prescribe one result for every dispute.[2]

This article asks how Articles 14, 19 and 21 work together to structure the protection of privacy, and whether the statutory architecture of the DPDP Act and the 2025 Rules raises questions under that constitutional framework. It adopts a doctrinal method: the primary materials are constitutional provisions, Supreme Court judgments, the DPDP legislation and rules, the Right to Information Act, and the GDPR. For the current status of litigation and EU legislative developments, it uses publicly accessible case trackers and official institutional records. Those procedural updates are date-sensitive and should be checked again against the relevant court or institutional docket at the time of publication.[3]

2. From divided authority to constitutional recognition

In *M.P. Sharma v Satish Chandra*, a Constitution Bench of eight judges considered search and seizure in the context of an Article 20(3) challenge. Its observations about the absence of a direct equivalent to the Fourth Amendment of the United States Constitution later became important in arguments against a general constitutional right to privacy. *Kharak Singh v State of Uttar Pradesh*, decided by a six-judge bench, invalidated night-time domiciliary visits under the relevant police regulation but rejected the broader claim that the Constitution recognised a general right to privacy. Subba Rao J.'s dissent gave greater weight to privacy as an aspect of personal liberty.[4]

Subsequent decisions developed the doctrine incrementally. *Gobind v State of Madhya Pradesh* proceeded on the assumption that privacy was constitutionally protected, while emphasising that the right could be subject to carefully justified State interests. *R. Rajagopal v State of Tamil Nadu* recognised protection against unauthorised publication of aspects of private life, subject to the applicable limits on privacy and freedom of expression. *People's Union for Civil Liberties v Union of India* treated telephone interception as an intrusion into privacy and prescribed procedural safeguards for interception under the Telegraph Act, 1885.[5]

In August 2017, the nine-judge bench in *Puttaswamy* unanimously held that privacy is a constitutionally protected fundamental right. The decision overruled *M.P. Sharma* and *Kharak Singh* to the extent that they were understood to deny such a right. The opinions differ in emphasis, but collectively describe privacy as a constitutional value connected with dignity, liberty, autonomy and the freedoms guaranteed by Part III. They also identify distinct dimensions of privacy, including bodily privacy, decisional privacy and informational privacy.[6]

Puttaswamy should be read with precision. It recognised a fundamental right and supplied the constitutional starting point; it did not declare all data collection unlawful, establish a universal right to secrecy, or decide in advance whether every subsequent statutory scheme is valid. The question after recognition is whether a particular interference has a lawful basis and can be justified within the Constitution's structure.

3. The constitutional structure: Articles 21, 19 and 14

3.1 Article 21: dignity, autonomy and personal liberty

Article 21 provides that no person shall be deprived of life or personal liberty except according to procedure established by law. After *Maneka Gandhi v Union of India*, that procedure cannot be treated as merely formal: it must be fair, just and reasonable. *Puttaswamy* placed privacy within this understanding of life and personal liberty. Privacy protects an individual's capacity to form intimate relationships, make personal

decisions and retain a sphere of life free from unjustified intrusion.[7]

The autonomy dimension can be seen in later constitutional decisions. *Navtej Singh Johar v Union of India* relied on dignity, autonomy and privacy in holding Section 377 of the Indian Penal Code unconstitutional insofar as it criminalised consensual sexual conduct between adults of the same sex. *Joseph Shine v Union of India* rejected the criminal offence of adultery and criticised a legal rule that subordinated a woman's sexual autonomy to the control of her husband. These cases are not simply data-protection decisions. They show that constitutional privacy concerns the conditions for personhood and choice, not only the confidentiality of information.[8]

Privacy remains qualified by other legally cognisable interests. In *Selvi v State of Karnataka*, the Supreme Court held that involuntary narco-analysis, polygraph and brain-mapping techniques violated protections relating to personal liberty and compelled testimony. In *Mr X v Hospital Z*, however, the Court accepted that disclosure of a patient's HIV-positive status to a prospective spouse could be justified in the circumstances before it. The latter decision should not be generalised into a broad power to disclose medical information; its significance is that privacy claims must be assessed against the rights and interests engaged by the particular facts.[9]

3.2 Article 19: privacy as a condition for other freedoms

Privacy also supports the meaningful exercise of Article 19 freedoms. Surveillance of communications, reading habits, associations or movements can deter lawful speech and association even where no formal prohibition is imposed. This chilling-effect concern is particularly important for journalists, political dissenters, researchers and people communicating with sources who may face retaliation. It does not follow that every surveillance measure violates Article 19; it follows that the effect on expression and association must be part of the constitutional assessment.

In *Anuradha Bhasin v Union of India*, the Supreme Court held that freedom of speech and expression through the internet receives protection under Article 19(1)(a), and that restrictions must satisfy constitutional requirements including proportionality and reviewability. In the Pegasus proceedings, *Manohar Lal Sharma v Union of India*, the Court ordered an independent technical inquiry into allegations of spyware use. The decision did not establish that every allegation had been proved. Its broader constitutional significance lies in the Court's refusal to treat national-security assertions as a categorical bar to judicial scrutiny and its recognition of the serious implications alleged surveillance may have for press freedom and civil liberties.[10]

3.3 Article 14: non-arbitrariness and equal protection

Article 14 contributes equality before the law and equal protection of the laws. In privacy disputes, it can matter where State action treats similarly situated persons differently without adequate justification, or where a law confers power without intelligible standards or meaningful review. *E.P. Royappa v State of Tamil Nadu* associated equality with the rejection of arbitrariness; *Shayara Bano v Union of India* later discussed the doctrine of manifest arbitrariness in reviewing legislation. The doctrine is not a free-standing licence to invalidate any policy with which a court disagrees. It requires analysis of the legal provision, its purpose, its structure and the relevant constitutional standard.[11]

The three Articles should therefore be read together, but not treated as interchangeable. Article 21 foregrounds personal liberty, dignity and autonomy; Article 19 makes visible the effect of surveillance and

data practices on protected freedoms; and Article 14 supplies a framework for testing unequal or arbitrary State power. The appropriate combination depends on the measure being challenged and the facts in the record.

4. The constitutional test for interference with privacy

Puttaswamy establishes that privacy is not absolute. The Supreme Court's later Aadhaar judgment applied a structured inquiry to State interference with privacy. The framework is commonly expressed through legality, a legitimate State aim, proportionality and procedural safeguards. These elements are best understood as a disciplined constitutional inquiry rather than as a mechanical checklist whose formulation was identical in every opinion.[12]

First, legality requires a valid legal basis. A serious interference should not rest solely on informal practice or unconstrained executive preference. Secondly, the State must identify a legitimate aim recognised by the constitutional order. Thirdly, proportionality requires a reasoned relationship between the measure and the aim pursued. The inquiry ordinarily considers whether the measure is suitable, whether a less restrictive but comparably effective alternative is available, and whether the benefits justify the burden on the right. Fourthly, safeguards matter because even a measure directed at a legitimate objective may be constitutionally defective if the risk of misuse is not adequately controlled.[13]

The proportionality principle was developed in Indian constitutional law in decisions including *Modern Dental College and Research Centre v State of Madhya Pradesh* and was applied to digital restrictions in *Anuradha Bhasin*. The Aadhaar judgment illustrates that the same constitutional analysis can yield different results across provisions: it upheld significant elements of the scheme while limiting the use of Aadhaar by private bodies in the manner then authorised by Section 57 of the Aadhaar Act. The lesson is neither that privacy always defeats State action nor that a stated public purpose automatically validates an intrusion. The legal basis, means, safeguards and evidentiary record remain central.[14]

5. Informational privacy, the State and private actors

Informational privacy concerns the collection, use, retention, disclosure and linkage of data relating to an identifiable person. A data set may disclose health, finances, relationships, movement, political activity or other intimate details, particularly when apparently ordinary records are combined. The Supreme Court recognised informational privacy as one dimension of the broader right in *Puttaswamy*. In *District Registrar and Collector v Canara Bank*, the Court also considered the privacy implications of State access to private records and rejected an unrestricted approach to inspection of banking documents.[15]

The constitutional position should not be overstated as a simple rule that every private data-processing dispute is directly an Article 21 claim. Fundamental rights primarily structure the relationship between individuals and the State, although the Constitution recognises some horizontal obligations and the Supreme Court has discussed the responsibility of non-State actors in privacy opinions. The direct constitutional route in a particular dispute must be distinguished from statutory duties, contract, tort, sectoral regulation and other legal remedies that may govern a private organisation's conduct. The DPDP Act is principally a statutory framework governing digital personal data processed by public and private entities within its scope.[16]

6. The DPDP Act and Rules: scope, structure and commencement

The DPDP Act, 2023, received presidential assent on 11 August 2023. It regulates digital personal data processed in India and, subject to the statutory conditions, processing outside India connected with offering goods or services to Data Principals within India. The Act uses the terms ‘Data Principal’, ‘Data Fiduciary’ and ‘Significant Data Fiduciary’, establishes the Data Protection Board of India, and provides for duties, individual rights, exemptions and monetary penalties. The Digital Personal Data Protection Rules, 2025, provide further detail on matters delegated by the Act.[17]

The commencement scheme is staggered. The Government’s notification G.S.R. 843(E), dated 13 November 2025, brought specified institutional and procedural provisions into force and prescribed later dates for other provisions. The Rules, notified as G.S.R. 846(E), likewise provide for different commencement dates: Rules 1, 2 and 17–21 take effect on publication; Rule 4 follows after one year; and Rules 3, 5–16, 22 and 23 follow after eighteen months. Accordingly, the framework should not be described as though every substantive obligation and every rule were already operative on the same date. The precise commencement position must be checked against the Gazette notification and any subsequent corrigendum or notification.[18]

The Act’s main architecture is significant. Sections 4–10 address grounds for processing and fiduciary obligations, including consent, certain legitimate uses, security safeguards and obligations relating to children and Significant Data Fiduciaries. Sections 11–14 specify rights of access to information about personal data, correction and erasure, grievance redressal and nomination. Section 16 addresses transfers outside India. Section 17 contains exemptions, while Sections 18–27 establish and describe the Data Protection Board and its powers. The Schedule sets maximum penalties for specified contraventions, including up to INR 250 crore for failure to maintain reasonable security safeguards and up to INR 200 crore for certain failures to notify a personal-data breach or comply with child-data obligations.[19]

7. Constitutional questions raised by the DPDP framework

7.1 State exemptions and law-enforcement processing

Section 17 distinguishes several categories of exempt processing. Section 17(1)(c) concerns processing in the interest of prevention, detection, investigation or prosecution of offences or contraventions of law. Section 17(2)(a) permits the Central Government to notify State instrumentalities for exemption on specified grounds, including sovereignty and integrity, security of the State, friendly relations with foreign States, public order and preventing incitement to certain offences. Section 7 separately identifies ‘certain legitimate uses’, including specified State functions. These provisions are legally distinct and should not be collapsed into a single, undifferentiated ‘State exemption’.[20]

The constitutional question is whether the breadth of an exemption, the conditions attached to it and the available review mechanisms satisfy the applicable standard in the circumstances. State interests such as national security and law enforcement can be legitimate. That proposition does not resolve whether a particular statutory category is sufficiently bounded, whether the measure is necessary, or whether safeguards adequately constrain the power. Conversely, the existence of an exemption does not by itself establish unconstitutionality. A court would need to examine the text, purpose, practical operation and surrounding legal safeguards.

7.2 Government information demands and confidentiality

Section 36 authorises the Central Government to call for information from the Board, a Data Fiduciary or an intermediary for prescribed purposes of the State. Rule 23(2) of the 2025 Rules addresses circumstances in which a Data Fiduciary or intermediary must not disclose the demand to a Data Principal where the specified national-security conditions are implicated. The concern raised by petitioners is that broad information-demand powers, when combined with confidentiality obligations, may weaken notice and independent scrutiny. The countervailing argument is that legitimate State functions can require confidential requests. The constitutional analysis must therefore focus on statutory precision, control over use, record-keeping, review and remedies, rather than relying on either proposition in the abstract.[21]

7.3 Section 44(3) and the Right to Information Act

Section 44(3) of the DPDP Act substituted a new Section 8(1)(j) in the Right to Information Act, 2005, referring to ‘information which relates to personal information’. The earlier clause linked the exemption to the relationship of information with public activity or interest, or to unwarranted invasion of privacy, and included a public-interest proviso. The amendment has therefore generated a substantial question about the balance between privacy and public access to information held by public authorities.[22]

That balance was central to CPIO, *Supreme Court of India v Subhash Chandra Agarwal*, in which the Supreme Court considered the interaction between privacy and the right to information under the earlier statutory wording. The amendment’s effect must be assessed against the current text, including the continuing operation of other RTI provisions such as Section 8(2), which contains a public-interest override, and Section 10, which provides for severability of exempt information. The existence of those provisions does not predetermine how they will operate after the amendment; nor does the amendment, without further analysis, answer every question about its constitutionality or practical effect.[23]

7.4 Regulatory independence and the enforcement model

The DPDP Rules provide for a search-cum-selection committee in the process for appointing the Chairperson and members of the Data Protection Board, with the Central Government making the appointment. Critics argue that this arrangement may give the executive substantial influence over a body expected to decide disputes involving data fiduciaries and, potentially, public authorities. The GDPR, by comparison, expressly requires supervisory authorities to act with complete independence. The difference is relevant to institutional design, but the two statutory regimes operate within different constitutional and administrative systems. A comparison cannot by itself establish that the Indian model is unconstitutional; the question is whether the statutory design meets the standards applicable under Indian law.[24]

Other design choices also merit analysis. The DPDP Act regulates digital personal data and does not create a separate statutory category equivalent to the GDPR’s special categories of personal data. It does not contain an express, general journalism exemption framed in the same way as Article 85 of the GDPR. It also does not create an express statutory compensation remedy for Data Principals comparable to a freestanding damages right under the GDPR, instead relying on the Board’s regulatory and penalty structure and the remedies available under other applicable law. These are comparative observations about statutory design; whether a particular difference is constitutionally invalid is a separate question.[25]

8. The European Union comparison: useful, but limited

The GDPR provides a useful comparator because it combines substantive data-protection rules with a rights framework and an institutional system of independent supervisory authorities. Its constitutional context includes Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, concerning respect for private and family life and protection of personal data. Article 8 of the European Convention on Human Rights is also relevant to the European human-rights framework. The GDPR sets out lawful bases for processing, special categories of data, rights of data subjects, restrictions under Article 23, cross-border transfer rules and administrative penalties.[26]

The Court of Justice of the European Union has developed this framework through decisions including *Digital Rights Ireland*, which invalidated the Data Retention Directive; *Google Spain*, which addressed the right to request de-referencing in particular circumstances; and *Schrems II*, which invalidated the EU-US Privacy Shield adequacy decision while maintaining the validity of standard contractual clauses subject to effective protection in practice. These decisions illustrate that data protection in the EU is not only a question of statutory obligations imposed on organisations; it is also tied to rights review and enforceable limits on public and private processing.[27]

In *Latombe v Commission*, the General Court dismissed an action seeking annulment of the European Commission's adequacy decision for the EU-US Data Privacy Framework on 3 September 2025. An appeal was lodged in Case C-703/25 P, which remains shown as pending in the Court of Justice's public case information as at 22 October 2026. Separately, the Commission's Digital Omnibus proposal, COM(2025) 837 final, was published in November 2025 and remains an ongoing legislative procedure in the official EU register. Neither the appeal nor the proposal should be presented as a final change to the law presently in force.[28]

The comparison should remain modest. It is reasonable to observe that the GDPR contains a more detailed catalogue of individual rights and stronger express requirements for supervisory independence. It is not accurate to assume that every GDPR rule can or should be transplanted into India, or that one legal system's design proves the constitutionality of the other. The comparison is most useful when it isolates institutional safeguards, limits on exceptions, transparency, remedies and review mechanisms that can be evaluated in the Indian constitutional setting.

9. The pending constitutional challenge

The constitutional challenge to the DPDP framework is led by *Venkatesh Nayak v Union of India*, W.P. (C) No. 177 of 2026, with connected petitions. Publicly accessible case material identifies challenges to Sections 17(1)(c), 17(2), 33(1), 36 and 44(3) of the Act and Rules 17 and 23(2) of the Rules, including arguments under Articles 14, 19(1)(a) and 21. These are petitioners' submissions, not findings of unconstitutionality.[29]

The public case tracker reports that notice was issued on 16 February 2026 and that the Court declined an interim stay at that stage. It records the matter as pending and lists a hearing on 7 August 2026. A specialist tracker last updated on 21 October 2026 reports that no challenged provision had been struck down or suspended and that interim applications remained unresolved in the latest public material it reviewed. These are secondary status reports, not a substitute for the Supreme Court's latest cause list and signed orders. The procedural position should be checked again immediately before publication, because a listing or order may change the position without extensive secondary reporting.[30]

Until a court orders otherwise, a pending constitutional challenge does not itself suspend a statute. However,

because commencement of the DPDP Act and Rules is staggered, the applicable obligations must be determined provision by provision and by reference to the operative Gazette notifications. It is therefore important not to confuse the legal status of the Act, the commencement date of any particular provision, and the merits of the pending challenge.[31]

10. Conclusion

Puttaswamy changed Indian privacy law by establishing that privacy is a fundamental right, not merely a statutory benefit or a matter of personal preference. Articles 21, 19 and 14 contribute distinct but related forms of protection: dignity and autonomy, the conditions for the exercise of speech and association, and a discipline against unequal or arbitrary State power. The proportionality framework requires a court to consider legality, legitimate aim, necessity, balancing and safeguards in light of the particular measure and evidence.

The DPDP Act is the next major test of how these principles apply to data governance. Its exemptions, information-demand powers, institutional design and amendment to the RTI Act raise questions that should be analysed carefully and without assuming the result. The pending proceedings make that analysis especially timely, but the parties' arguments must not be reported as judicial holdings. The GDPR offers a useful comparative lens for considering rights, remedies and institutional independence; it does not resolve the constitutional question in India.

The central proposition is therefore deliberately limited. Privacy is not a trump card against every public measure, and a legitimate public purpose is not a complete answer to every privacy objection. The constitutional task is to test the actual legal authority, purpose, necessity, proportionality and safeguards of the interference. That is what makes privacy a practical constitutional standard rather than merely a setting on a device.

Table of Cases

Anuradha Bhasin v Union of India (2020) 3 SCC 637.

CPIO, Supreme Court of India v Subhash Chandra Agarwal (2020) 5 SCC 481.

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18) EU:C:2020:559.

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (Joined Cases C-293/12 and C-594/12) EU:C:2014:238.

District Registrar and Collector, Hyderabad v Canara Bank (2005) 1 SCC 496.

E P Royappa v State of Tamil Nadu (1974) 4 SCC 3.

Gobind v State of Madhya Pradesh (1975) 2 SCC 148.

Google Spain SL v Agencia Española de Protección de Datos (AEPD) (C-131/12) EU:C:2014:317.

Joseph Shine v Union of India (2019) 3 SCC 39.

Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295; (1964) 1 SCR 332.

Latombe v Commission (Case T-553/23) EU:T:2025:831; appeal, Case C-703/25 P (pending).

M P Sharma v Satish Chandra AIR 1954 SC 300; (1954) SCR 1077.

Maneka Gandhi v Union of India (1978) 1 SCC 248.

Manohar Lal Sharma v Union of India (Pegasus) (2022) 3 SCC 551.

Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353.

Mr X v Hospital Z (1998) 8 SCC 296.

Navtej Singh Johar v Union of India (2018) 10 SCC 1.

People's Union for Civil Liberties v Union of India (1997) 1 SCC 301.

K S Puttaswamy (Aadhaar) v Union of India (2019) 1 SCC 1.

Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632.

Selvi v State of Karnataka (2010) 7 SCC 263.

Shayara Bano v Union of India (2017) 9 SCC 1.

Legislation and Instruments

Constitution of India 1950, arts 14, 19 and 21.

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, s 57 (as considered in the 2018 Aadhaar judgment).

Digital Personal Data Protection Act 2023 (Act 22 of 2023). Official text: <https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf>

Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), 13 November 2025 (commencement of the DPDP Act). Official Gazette: <https://egazette.gov.in/WriteReadData/2025/267647.pdf>

Digital Personal Data Protection Rules 2025, G.S.R. 846(E), 13 November 2025. Official Gazette: <https://egazette.gov.in/WriteReadData/2025/267650.pdf>

Right to Information Act 2005, ss 8(1)(j), 8(2) and 10.

Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.

Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7, 8 and 52.

European Commission, Proposal for a Regulation on the simplification of the digital legislative framework (Digital Omnibus), COM(2025) 837 final, 19 November 2025. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837>

Research and status sources

Supreme Court Observer, "Constitutionality of the Digital Personal Data Protection Act, 2023" (case tracker,

last updated 7 August 2026), <https://www.scobserver.in/cases/constitutionality-of-the-digital-personal-data-protection-act-2023/> (accessed 22 October 2026).

Abhijeet Singh, “Supreme Court challenge to the DPDP Act: what stands today” (dpdprules.org, updated 21 October 2026), <https://dpdprules.org/blog/dpdp-act-supreme-court-challenge> (accessed 22 October 2026). Used only for procedural status; primary court records remain authoritative.

Court of Justice of the European Union, “Latombe v Commission” (Case C-703/25 P), case information page, [https://infocuria.curia.europa.eu/tabs/affair?](https://infocuria.curia.europa.eu/tabs/affair?lang=EN&publishedId=C-703%2F25+P&searchTerm=%22T-553%2F23%22)

[lang=EN&publishedId=C-703%2F25+P&searchTerm=%22T-553%2F23%22](https://infocuria.curia.europa.eu/tabs/affair?lang=EN&publishedId=C-703%2F25+P&searchTerm=%22T-553%2F23%22) (accessed 22 October 2026).

EUR-Lex, Procedure 2025/0360/COD, COM(2025) 837 final (Digital Omnibus), https://eur-lex.europa.eu/procedure/EN/2025_360 (accessed 22 October 2026).

Notes

1. Constitution of India 1950, arts 14, 19 and 21; Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
2. M P Sharma v Satish Chandra AIR 1954 SC 300; (1954) SCR 1077; Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295; (1964) 1 SCR 332; Gobind v State of Madhya Pradesh (1975) 2 SCC 148; R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632; People’s Union for Civil Liberties v Union of India (1997) 1 SCC 301.
3. Methodological note: primary legal materials are distinguished from secondary reporting. The pending DPDP proceedings are discussed as reported procedural developments, not as adjudicated findings. Current procedural status is time-sensitive and was checked against publicly accessible case trackers on 22 October 2026.
4. M P Sharma v Satish Chandra AIR 1954 SC 300; (1954) SCR 1077; Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295; (1964) 1 SCR 332.
5. Gobind v State of Madhya Pradesh (1975) 2 SCC 148; R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632; People’s Union for Civil Liberties v Union of India (1997) 1 SCC 301.
6. Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (Supreme Court of India) <https://api.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf>.
7. Maneka Gandhi v Union of India (1978) 1 SCC 248; Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
8. Navtej Singh Johar v Union of India (2018) 10 SCC 1; Joseph Shine v Union of India (2019) 3 SCC 39.
9. Selvi v State of Karnataka (2010) 7 SCC 263; Mr X v Hospital Z (1998) 8 SCC 296.
10. Anuradha Bhasin v Union of India (2020) 3 SCC 637; Manohar Lal Sharma v Union of India, 2021 INSC 682 (order dated 27 October 2021). The latter concerned allegations of spyware use and the constitution of an independent technical committee; it should not be read as a finding that every alleged infection was proved.
11. E P Royappa v State of Tamil Nadu (1974) 4 SCC 3; Shayara Bano v Union of India (2017) 9 SCC 1.
12. Justice K S Puttaswamy (Aadhaar) v Union of India (2019) 1 SCC 1. The Court applied proportionality in reviewing the Aadhaar architecture; the opinions in Puttaswamy (Privacy) and the later Aadhaar judgment should be read individually and in context.
13. Justice K S Puttaswamy (Aadhaar) v Union of India (2019) 1 SCC 1; Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353.
14. Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353; Anuradha Bhasin v Union of India (2020) 3 SCC 637; Justice K S Puttaswamy (Aadhaar) v Union of India (2019) 1 SCC 1.
15. Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1; District Registrar and Collector, Hyderabad v Canara Bank (2005) 1 SCC 496.
16. Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, especially the separate opinions addressing non-State actors; Digital Personal Data Protection Act 2023, ss 3–4 and 17. The extent of direct horizontal application of the

privacy right is not treated here as a single settled rule for all private disputes.

17. Digital Personal Data Protection Act 2023 (Act 22 of 2023), ss 1–4, 8–18. Official text: <<https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf>> accessed 22 October 2026.

18. Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), 13 November 2025 (commencement of the Digital Personal Data Protection Act 2023), <<https://egazette.gov.in/WriteReadData/2025/267647.pdf>> accessed 22 October 2026; Digital Personal Data Protection Rules 2025, G.S.R. 846(E), 13 November 2025, r 1, <<https://egazette.gov.in/WriteReadData/2025/267650.pdf>> accessed 22 October 2026. Check the Gazette and any later corrigendum before relying on a particular commencement date.

19. Digital Personal Data Protection Act 2023, ss 4–17, 18–27, 33–36 and the Schedule.

20. Digital Personal Data Protection Act 2023, ss 7 and 17(1)(c), 17(2)(a). Section 17(1)(c) concerns processing for prevention, detection, investigation or prosecution of an offence or contravention of law; s 17(2)(a) concerns notified State instrumentalities on specified grounds.

21. Digital Personal Data Protection Act 2023, s 36; Digital Personal Data Protection Rules 2025, r 23(2). The constitutional objections described in the text are arguments advanced by petitioners in the pending challenge, not findings of the Court.

22. Digital Personal Data Protection Act 2023, s 44(3), amending Right to Information Act 2005, s 8(1)(j). The amendment is among the provisions notified to commence with effect from the 2025 commencement notification.

23. CPIO, Supreme Court of India v Subhash Chandra Agarwal (2020) 5 SCC 481; Right to Information Act 2005, ss 8(2) and 10. Subhash Chandra Agarwal interpreted the prior statutory framework; its reasoning remains relevant to the balance of interests but must be distinguished from the amended wording.

24. Digital Personal Data Protection Rules 2025, r 17; Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 51–52.

25. Digital Personal Data Protection Act 2023, ss 11–14, 17 and 33–34; Regulation (EU) 2016/679, arts 9 and 85. The comparison concerns statutory text and structure; possible constitutional consequences require separate analysis.

26. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 6–9, 15–23, 44–49, 51–52 and 83; Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7, 8 and 52; European Convention on Human Rights, art 8.

27. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (Joined Cases C-293/12 and C-594/12) EU:C:2014:238; Google Spain SL v Agencia Española de Protección de Datos (AEPD) (C-131/12) EU:C:2014:317; Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (C-311/18) EU:C:2020:559.

28. *Latombe v Commission* (Case T-553/23) EU:T:2025:831; appeal, Case C-703/25 P (pending as shown in the Court of Justice case information page on 22 October 2026), <<https://infocuria.curia.europa.eu/tabs/affair?lang=EN&publishedId=C-703%2F25+P&searchTerm=%22T-553%2F23%22>> accessed 22 October 2026; European Commission, Proposal for a Regulation on the simplification of the digital legislative framework (Digital Omnibus), COM(2025) 837 final, 19 November 2025, procedure 2025/0360/COD, <https://eur-lex.europa.eu/procedure/EN/2025_360> accessed 22 October 2026.

29. Venkatesh Nayak v Union of India, W.P. (C) No. 177 of 2026, writ petition and case materials available via Supreme Court Observer, <<https://www.scobserver.in/cases/constitutionality-of-the-digital-personal-data-protection-act-2023/>> accessed 22 October 2026.

30. Supreme Court Observer, ‘Constitutionality of the Digital Personal Data Protection Act, 2023’ (last updated 7 August 2026), <<https://www.scobserver.in/cases/constitutionality-of-the-digital-personal-data-protection-act-2023/>> accessed 22 October 2026; Abhijeet Singh, ‘Supreme Court challenge to the DPDP Act: what stands today’ (dpdprules.org, updated 21 October 2026), <<https://dpdprules.org/blog/dpdp-act-supreme-court-challenge>> accessed 22 October 2026. Both are secondary procedural sources; verify the latest signed order and cause list before publication.

31. Digital Personal Data Protection Act 2023, s 1(2); Notification G.S.R. 843(E), 13 November 2025; Digital Personal Data Protection Rules 2025, r 1. These instruments prescribe staggered commencement; the date applicable to each provision should be checked against the Gazette text and subsequent notifications.

Bibliography / references

Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (Supreme Court of India) <https://api.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf>.

Copyright: Yuvraj | Publisher: The Legal Gazette | Licence: Creative Commons Attribution-ShareAlike 4.0 <https://creativecommons.org/licenses/by-sa/4.0/>. Publication permissions: I grant The Legal Gazette a non-exclusive, worldwide licence to publish, host, distribute, display, and archive my article, subject to the selected licence and applicable third-party rights. I retain copyright ownership.. Exclusivity: Exclusive. Additional academic author consent: contact-first.

Common case, legislation, book, journal and web templates; jurisdiction-specific abbreviations, special authorities and complex cross-references require editorial checking. Formatting does not verify a source.
Academic reuse: Academic Reuse Policy applies subject to the article licence, copyright, attribution and any required author consent. See thelegalgazette.org/#writing-policy.