Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Data Protection, Personal Autonomy and Article 21: Emerging Constitutional Challenges in India

Anurag Kamboj[1], Dr. Syed Irfan Ali[2]

[1]LL.M. Student, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India
[2]Associate Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.

DOI: https://doi.org/10.63363/aijfr.2026.v07i06.8972

Abstract

The current study is an examination of the constitution's journey with respect to the right to privacy and personal autonomy under Article 21 of the Constitution of India especially since the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) recognized privacy as a fundamental right.[1] It highlights how Article 21 became more and more restrictive in its interpretation from a judgment in Kharak Singh[2] to a series of nine-judge bench rulings to reach the stage where informational and decisional autonomy will be recognized in law, theoretically, and in execution, as well as the legislative attempt and action in formulating the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025[3] which are expected to come into operation in November 2025. Subsequently, the paper explores in detail several rising constitutional flash points that pose practical questions related to the Puttaswamy interpretation, such as: the Supreme Court challenge to the exemption regime in the Act, and the amendment to the Indian Right to Information Act[4]; the autonomy of the Data Protection Board of India; children's informational autonomy (APAAR litigation)[5]; and the judicial adjudication of a right to be forgotten[6]; and the extension of Article 21 to digital access.[7] It relies on case law to date, up to November 2026, to show that the Indian movement towards privacy rights has shifted from being declaratory to an implementation one, where the proportionality doctrine set out in

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 : AIR 2017 SC 4161 [hereinafter *Puttaswamy*].

[2] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 : (1964) 1 SCR 332 [hereinafter *Kharak Singh*].

[3] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023) [hereinafter DPDP Act]; The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), dated 13 Nov. 2025 [hereinafter DPDP Rules].

[4] The Right to Information Act, 2005 (Act 22 of 2005), s. 8(1)(j) [hereinafter RTI Act], as amended by DPDP Act, *supra* note 3, s. 44(3).

[5] *Abhishek Baxi & Ors. v. Union of India & Ors.*, W.P.(C) No. 832 of 2026, 2026 SCC OnLine SC 1391 (Supreme Court of India, decided 20 July 2026) [hereinafter *Abhishek Baxi*].

[6] *Laksh Vir Singh Yadav v. Union of India & Ors. and Connected Matters*, W.P.(C) 1021/2016 & Connected Matters, 2026:DHC:4891 (Delhi High Court, decided 29 May 2026) [hereinafter *Laksh Vir Singh Yadav*].

[7] *Amar Jain v. Union of India*; *Pragya Prasun v. Union of India*, W.P.(C) No. 49 of 2025 & W.P.(C) No. 289 of 2024 (Supreme Court of India, decided 30 Apr. 2025) [hereinafter *Amar Jain*].

Puttaswamy is being applied to other constitutional values of transparent, secure and efficient administration.

Keywords: Article 21, Right to Privacy, Personal Autonomy, Informational Self-Determination, Digital Personal Data Protection Act 2023, *Puttaswamy*, Data Protection Board, Constitutional Law

1. Introduction

Over the last ten years, India's constitutional experience and engagement with personal data has undergone a significant transformation: At the same time as the country's digital systems have expanded unparalleled, in unprecedented ways — to enrol over a billion citizens into Aadhaar[8], to launch Uniformed Payments Interface and to extend digital personal identity into services and areas associated with education, health, and welfare delivery, via schemes such as the Automated Permanent Academic Account Registry (APAAR)[9] — there has also been a judicial and legislative reckoning. Article 21 of the Constitution that states “No person shall be denied life or personal liberty except in accordance with the procedure provided by law”[10] sits at the heart of this reckoning. Article 21 has since been understood not as a stringent formal right but the substantive haven of a growing list of unenumerated rights; and personal autonomy, which this encompasses, is perhaps the most significant recent addition to that list, over the course of the last ten years.

The watershed judgment was that of Justice K.S. Puttaswamy (Retd.) v. Union of India in which a 9-judge bench of the Supreme Court unanimously declared that privacy is part of Article 21 and in essence of freedoms enumerated under Part III in general.[11] The Court's decision more than just solved a "controversial question" of interpreting the meaning of the two clauses, it also provided a "normative vacuum" in the Indian law of processing personal data, which in one sense or the other, compelled the State to enact a data protection law. It came, after some delays, in the form of the Digital Personal Data Protection Act, 2023 ("DPDP Act") and Rules of 2025 (the Rules), respectively issued in November 2025 – almost exactly nine years after the decision in Puttaswamy.[12]

This paper looks at that nine-year period, but with a focus on the changes that have occurred in the wake of that. As provisions of the DPDP Act come into play as statute and become operative as law, constitutional guarantees including that of Puttaswamy are now getting tested, proposition by proposition, in a series of litigation battles that played out in 2025 and 2026, starting with the scope and extent of the Government's exemptions from the DPDP Act itself[13]; then the controversial amendment of the Right to Information Act, 2005 by the DPDP Act[14]; the independence of the newly constituted Data Protection Board of India[15]; whether children's data is covered by the DPDP Act or not for schemes such

[8] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act 18 of 2016) [hereinafter Aadhaar Act].

[9] *Abhishek Baxi*, *supra* note 5; *see infra* Part VII(D).

[10] The Constitution of India, 1950, art. 21.

[11] *Puttaswamy*, *supra* note 1.

[12] DPDP Act, *supra* note 3; DPDP Rules, *supra* note 3. The nine-Judge Bench delivered its judgment on 24 Aug. 2017: *Puttaswamy*, *supra* note 1.

[13] DPDP Act, *supra* note 3, s. 17; *see infra* Part VII(A).

[14] RTI Act, *supra* note 4, s. 8(1)(j); DPDP Act, *supra* note 3, s. 44(3); *see infra* Part VII(B).

[15] DPDP Act, *supra* note 3, ss. 18–19; *see infra* Part VII(C).

as APAAR[16]; whether the Puttaswamy right can be extended to digital access[17]; etc. These conflicts are part of the new constitutional conflicts for which this paper provides its title. There are three movements to the paper. Part III shows the doctrinal development of article 21 privacy jurisprudence from a restrictive phase to the Puttaswamy synthesis and part IV illustrates the convergence of the right to equality in the matter. The conceptual content of the value of Personal Autonomy, as interpreted through the eyes of the law are explored in Parts V and VI, which dissect the legislative synthesis into the DPDP Act and Rules. Part VII reviews each of the flash points which have arisen since the Act came into force, Part VIII provides an analysis in a critical sense and Part IX brings this work to a conclusion.

2. Literature Review

In Indian constitutional scholarship, there are two main broad bodies of work which can be distinguished both by time and substance as to the study of privacy under the Indian Constitution. Prior to 2017, legal pronouncements in the murky and scattered terrain of the texts examined wrote off privacy rights in distinct situations without deciding when and under what conditions privacy will be regarded as a standalone fundamental right.[18] Puttaswamy removed the doctrinal fragility that was highlighted in this literature, which were correct in singling it out as such and concluded that it could be solved only by a nine-judge bench.[19]

A second much larger body of scholarship that focussed on the substance of the doctrine of Puttaswamy per se, namely on many concurrent opinions,[20] the formulation of a proportionality doctrine and the following of the landmark 2018 Aadhaar judgment.[21] This literature has been useful in theory, the design of which was considered to be the creation of a new constitution, but for the most part, it treated the DPDP Act, 2023, as the end of the theory,[22] that is as the conclusion of a constitutional struggle that began with the Puttaswamy judgement. What is impossible to do at this point is to comment on the additional flow of litigation against the DPDP Rules, 2025, that was introduced following the notification in November 2025,[23] the interplay with the right to information, and/or use of administrative schemes in scenarios involving children's data. This paper aims to fill this gap by examining the doctrinal evolution of Article 21 privacy jurisprudence, supplemented by analysis of the specific constitutional challenges that occurred in the first year of operational DPDP Act, using judicial orders and rule-making as a guidepost until November 2026.

[16] *Abhishek Baxi*, *supra* note 5; *see infra* Part VII(D).

[17] *Amar Jain*, *supra* note 7; *see infra* Part VII(F).

[18] *See* Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography", 26 NLSI Rev. 127 (2014).

[19] *Puttaswamy*, *supra* note 1; *see also K.S. Puttaswamy v. Union of India*, (2015) 8 SCC 735 (order of reference to a larger Bench) [hereinafter *K.S. Puttaswamy (Reference)*].

[20] *See, e.g.*, Vrinda Bhandari, Amba Kak, Smriti Parsheera & Faiza Rahman, "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict", IndraStra Global (2017).

[21] *K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1 [hereinafter *Aadhaar Judgment*].

[22] DPDP Act, *supra* note 3.

[23] DPDP Rules, *supra* note 3.

3. Article 21 and the Constitutional Journey of Privacy

The nature of privacy as a constitutional interest in India was left unclear through the second part of the 1970s, the first quarter of the 1980s, the last ten years of the 1990s, and the first half of the 2010s. In M.P. Sharma vs. Satish Chandra[24], an eight-judge bench said that the constitutional right to privacy does not extend to the power of search and seizure as granted by the Code of Criminal Procedure,[25] since constitutional framers "deliberately" chose to not incorporate it into the Constitution in the American style.[26] In another judgment, similar scepticism was seen in Kharak Singh v. State of Uttar Pradesh, in which a six-judge bench of the Court ruled that an Uttar Pradesh government police regulation allowing night-time visits to the residence of "history sheeters" was unconstitutional and did not allow a general constitutional right to privacy to be recognised.[27] It was left for Subba Rao, J., in dissent, to predict the day of the change in doctrine, which had been cast as personal liberty, including the freedom from unauthorised entry into a person's home and person, being a "compendious term".[28]

Only when the case of Maneka Gandhi v. Union of India[29] finally ditched the narrow and compartmentalised interpretation of interpretation of fundamental rights which had informed A.K. Gopalan v. State of Madras[30] in the year 1982, did the Supreme Court hold that the "procedure established by law" under Article 21 must be fair, just and reasonable and that the Articles 14, 19 and 21 constituted an interlocking 'golden triangle'.[31] This doctrinal change set up the birth site that permitted the subsequent development of privacy rights in court. In Govind v. State of Madhya Pradesh[32], the Court upheld the police surveillance policies but for the first time, recognised that there is a right to privacy that can be found in Article 21, provided the state reasons with a compelling state interest.[33] In R. Rajagopal v. State of Tamil Nadu[34], the Court went further and said that there is a right to privacy as an integral part of the right to life, which also includes a qualified "right to be let alone,"[35] in relation to the unauthorised publication of information regarding a convict. In People's Union for Civil Liberties v Union of India[36], it set this out going through to the act of surveillance of telephones; and the presence of a 'just, fair and reasonable' procedure was therefore necessary for Article 21 to hold true.[37]

Indian courts by the beginning of the 2010s had granted rights to privacy in limited contexts – the home, reputation and telephonic communication – without establishing it as a fundamental right but successive governments' counsel had become deft at exploiting the vacuum between the fundamental rights, with

[24] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 : 1954 SCR 1077 [hereinafter *M.P. Sharma*].

[25] The Code of Criminal Procedure, 1898 (Act 5 of 1898), ss. 94, 96.

[26] *M.P. Sharma*, *supra* note 24 (declining to read into the Constitution a protection analogous to the Fourth Amendment to the U.S. Constitution).

[27] *Kharak Singh*, *supra* note 2 (impugning Regulation 236 of the Uttar Pradesh Police Regulations).

[28] *Ibid.* (Subba Rao, J., dissenting).

[29] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 : AIR 1978 SC 597 [hereinafter *Maneka Gandhi*].

[30] *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27 : 1950 SCR 88.

[31] *Maneka Gandhi*, *supra* note 29; The Constitution of India, 1950, arts. 14, 19, 21.

[32] *Govind v. State of Madhya Pradesh*, (1975) 2 SCC 148 : AIR 1975 SC 1378.

[33] *Ibid.*

[34] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 : AIR 1995 SC 264.

[35] *Ibid.*

[36] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568.

[37] *Ibid.*

the issue of correctness of the Sharma and Kharak Singh judgments[38] most pointedly being raised during the early proceedings in the Aadhaar litigation[39] before the Union counsel pleaded that it would be appropriate to set aside such correctness before going to the constitutionality of Aadhaar in a hearing of sufficient strength. That referral resulted in the nine-judge bench which was the subject of the next Part.[40]

4. Puttaswamy and the Doctrinal Foundations of Informational Privacy and Autonomy

The nine-judge Bench reached the unanimous decision in Justice K.S. Puttaswamy v. Union of India on 24 August 2017 that the "right to privacy" is encompassed in the concept of Article 21 and is "implied" in Part III, the freedoms as a whole.[41] The Court has expressly rebutted the reasoning of M.P. Sharma and the majority in Kharak Singh, the dissenting opinion of J. over 5 decades ago.[42] Although unanimous in a judgment, there were six separate opinions, mainly by Chandrachud, J.[43] It is noteworthy that while four of them (Abeler, Chelameswar, Bobde, Nariman and Sapre & Kaul, JJ) delivered their opinions separately, their thoughts together form the doctrinal language used in almost all privacy cases in India to date.

Here three strands of that reasoning are of predominant importance. To begin with, the Court did not define privacy as a single concept: it considered privacy as being of different facets, such as "bodily or physical privacy, decisional privacy, (the ability to make intimate personal choices about sexual orientation, marriage, and reproduction), and informational privacy, (the right to control dissemination of personal data)."[44] Second, acknowledging the right to "informational self-determination," as the German Constitutional Court did in its census decision,[45] as a part of the principle of Article 21: that "the person has a constitutionally-guaranteed interest in controlling the collection, processing and use of information about herself, even after a "constructive measure" of voluntary disclosure for a certain purpose. Third, the Court laid down a well-sculpted test for a state measure which interferes with privacy – the measure must be legally upheld, pursue a state aim, be necessary and must use the least restrictive means possible including adequate procedural safeguards which prevent abuse of such interference,[46] Kaul, J. added a fourth requirement that the measure is adequately protected and secured from misuse.[47] This four-part key framework: legality, legitimate aim, proportionality and procedural safeguards, has since been adopted in privacy cases2 of all significance and will be repeated in every significant privacy action since then, as Part VII demonstrates.[48]

[38] *M.P. Sharma*, *supra* note 24; *Kharak Singh*, *supra* note 2.

[39] *K.S. Puttaswamy (Reference)*, *supra* note 19.

[40] *Puttaswamy*, *supra* note 1; *see infra* Part IV.

[41] *Puttaswamy*, *supra* note 1 (opinion of Chandrachud, J.).

[42] *Puttaswamy*, *supra* note 1 (overruling *M.P. Sharma*, *supra* note 24, and the majority opinion in *Kharak Singh*, *supra* note 2, to the extent that they held privacy not to be a fundamental right).

[43] *Puttaswamy*, *supra* note 1 (opinions of Chandrachud, J., for himself, Khehar, C.J., Agrawal and Nazeer, JJ.; Chelameswar, J.; Bobde, J.; Nariman, J.; Sapre, J.; and Kaul, J.).

[44] *Puttaswamy*, *supra* note 1 (opinion of Chandrachud, J.).

[45] Judgment of 15 Dec. 1983, 65 BVerfGE 1 (Ger.) (*Census Case*); *see generally Puttaswamy*, *supra* note 1.

[46] *Puttaswamy*, *supra* note 1 (opinions of Chandrachud, J. and Kaul, J.).

[47] *Puttaswamy*, *supra* note 1 (opinion of Kaul, J.).

[48] *See infra* Part VII.

More importantly, in several opinions, Puttaswamy expressed its views that there was no comprehensive data protection law in existence and highlighted that in the era of digital technology, possession of such law was more than a constitutional need, it was an imperative.[49] A year later, in the Aadhaar judgment K.S. Puttaswamy v. Union of India (2019) 1 SCC 1[50] in which a majority of five benchers affirmed the fundamental architecture of Aadhaar in the form of a proportionate mechanism for ensuring targeted delivery of welfare subsidies, ancillary provisions – such as linking of Aadhaar with bank accounts and mobile connections, and the private commercialization of Aadhaar authentication under what is now no longer available Section 57[51] – were struck down, and importantly for future litigations referred in Part VII, the Bench had held that once again that children cannot be compelled to enrol in Aadhaar without the informed consent of their parent or guardian, and that benefits cannot be denied to a child on grounds of non-conformance with Aadhaar.[52] Such reasoning was used by the Court in other areas too – in the case of Navtej Singh Johar v. Union of India,[53] it relied on the autonomy strand of Puttaswamy's to recognize sexual orientation as an attribute of privacy and dignity, as the basis for decriminalizing consensual same-sex conduct under Section 377 IPC;[54] in Joseph Shine v. Union of India,[55] it relied on the autonomy strand of Puttaswamy's to strike down the offence of adultery.[56] Together, these cases should place "personal autonomy" firmly within the scope of Article 21 dignity case law as a specifically worked-out dimension of dignity, consisting of a body, decisional, and information component, which this paper proposes in Part VI.

5. The Legislative Response: From the Srikrishna Committee to the DPDP Act, 2023 and Rules, 2025

Puttaswamy wasn't exaggerating when he said there is a 'normative vacuum'.[57] The Union government had in July 2017 set up a Committee of Experts on Data Protection headed by Justice B.N. Srikrishna[58] to come up with a complete blueprint for a legislation on data protection. In July 2018, the Committee had presented its report, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, and the draft Personal Data Protection Bill, 2018.[59] The drafts were designed on a European appearance basically, the EU General Data Protection Regulation,[60] a significant, rights-centred framework, with an

[49] *Puttaswamy*, *supra* note 1.

[50] *Aadhaar Judgment*, *supra* note 21.

[51] Aadhaar Act, *supra* note 8, s. 57; *Aadhaar Judgment*, *supra* note 21 (striking down s. 57 to the extent that it permitted private entities to seek authentication).

[52] *Aadhaar Judgment*, *supra* note 21.

[53] *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1 : AIR 2018 SC 4321.

[54] The Indian Penal Code, 1860 (Act 45 of 1860), s. 377 [hereinafter IPC].

[55] *Joseph Shine v. Union of India*, (2019) 3 SCC 39 : AIR 2018 SC 4898.

[56] IPC, *supra* note 54, s. 497; The Code of Criminal Procedure, 1973 (Act 2 of 1974), s. 198(2).

[57] *Puttaswamy*, *supra* note 1.

[58] Committee of Experts on Data Protection (Chair: Justice B.N. Srikrishna), *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, July 2018) [hereinafter *Srikrishna Committee Report*].

[59] *Srikrishna Committee Report*, *supra* note 58 (annexing the Personal Data Protection Bill, 2018).

[60] 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

independent Data Protection Authority, purpose limitation, data localisation, and an extensive checklist of data-principal rights.

Srikrishna Committee suggested its recommendations as law in original form. In December 2019, a revised Personal Data Protection Bill, 2019 was introduced in the Lok Sabha[61] and was referred to a Joint Parliamentary Committee (JPC), which it has been sitting as since December 2019, and reports only in December 2021 along with recommendations and amendments, including regulation of non-personal data.[62] By that point the Bill was subject to sustained criticism from civil liberties groups for the scope of government exemptions, as well as the compliance burden from industry, and the government dropped plans to introduce it altogether in August 2022,[63] with a commitment to developing a "comprehensive legal framework". It took the form of two bills: the draft Digital Personal Data Protection Bill, 2022, a simple draft that was put out for consultation in November 2022,[64] and the Digital Personal Data Protection Bill, 2023, which was introduced in the Lok Sabha on 3 August 2023, and passed two days later and by the Rajya Sabha on 9 August 2023, before it received presidential assent on 11 August 2023[65] — just under six years after the Srikrishna Committee was formed and the Puttaswamy bench was first constituted.

The DPDP Act is patterned on the GDPR,[66] but departs from it in a number of ways that are pertinent to the analysis in Part VII. It relates to digital personal data processed in India, and extraterritorially when processing outside India is in relation to the offer of goods or services to data principals in India.[67] It focuses on the relationship between a person that determines the purpose and the means of processing (Data Fiduciary) and the person concerned (Data Principal),[68] with extended obligations for those whose volume and sensitivity of data processed "significantly", are notified as "Significant Data Fiduciaries".[69] Only free, specific, informed, unconditional and unambiguous consent, expressed in concrete and affirmative action, or one of a number of "certain legitimate uses" set out in Section 7,[70] is acceptable for processing; and, importantly, processing for the provision of any subsidy, benefit, service, certificate, licence or permit by the State does not require consent at all.[71] There is no mechanism in law to review such exemption of substantive obligations independently and there is an exemption to most of the substantive obligations of government processing in a chapter extending to a length of four pages in the statute, for the purpose of sovereign security, security of the State, public order etc.[72] In Chapter V, penalties - in hundreds of crores of rupees - have been delegated to a Data Protection Board of India,

[61] The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019).

[62] Joint Committee on the Personal Data Protection Bill, 2019, *Report* (Seventeenth Lok Sabha, Lok Sabha Secretariat, Dec. 2021).

[63] The Bill was withdrawn from the Lok Sabha on 3 Aug. 2022.

[64] Ministry of Electronics and Information Technology, *The Digital Personal Data Protection Bill, 2022* (draft for public consultation, 18 Nov. 2022).

[65] DPDP Act, *supra* note 3; *see also* PRS Legislative Research, "Digital Personal Data Protection Bill, 2023" (Bill No. 113 of 2023), *Bill Summary* (2023).

[66] GDPR, *supra* note 60.

[67] DPDP Act, *supra* note 3, s. 3.

[68] DPDP Act, *supra* note 3, s. 2 (defining "Data Fiduciary" and "Data Principal").

[69] DPDP Act, *supra* note 3, ss. 2(z), 10.

[70] DPDP Act, *supra* note 3, ss. 4, 6(1), 7.

[71] DPDP Act, *supra* note 3, s. 7(b).

[72] DPDP Act, *supra* note 3, s. 17.

with its members being appointed by the Central Government on the recommendation of a search-cum-selection committee, which is also largely comprised of government nominees.[73]

It took nearly as long as the Act itself to get the Implementing Rules. A draft Digital Personal Data Protection Rules, 2025 has been issued for comments on 3 January 2025[74] while the final Digital Personal Data Protection Rules, 2025 was notified on 13–14 November 2025 along with a notification establishing a four-member Data Protection Board of India with its headquarters in the National Capital Region.[75] The Rules are not one-size-fits-all; instead, there is a staggered rollout, organised in three phases, detailed in Table I.[76]

Table I: Legislative and Regulatory Timeline of India's Data Protection Framework[77]

Date	Development
July 2017	Committee of Experts on Data Protection constituted under Justice B.N. Srikrishna
24 August 2017	*Puttaswamy* (2017) recognizes privacy as a fundamental right under Article 21
July 2018	Srikrishna Committee report and draft Personal Data Protection Bill, 2018 submitted
December 2019	Personal Data Protection Bill, 2019 introduced; referred to Joint Parliamentary Committee
August 2022	Personal Data Protection Bill, 2019 withdrawn from Parliament
November 2022	Draft Digital Personal Data Protection Bill, 2022 released for consultation
11 August 2023	Digital Personal Data Protection Act, 2023 receives presidential assent
3 January 2025	Draft Digital Personal Data Protection Rules, 2025 released for consultation
13–14 November 2025	DPDP Rules, 2025 notified; Data Protection Board constituted; first enforcement phase begins
13–14 November 2026	Second enforcement phase, covering core compliance obligations, takes effect
14 May 2027	Final enforcement phase scheduled to take effect

As of the time of this writing, the first of these three phases has officially begun, and the second has begun as of this week,[78] bringing the DPDP framework to a uniquely informative moment: it's not quite

[73] DPDP Act, *supra* note 3, ss. 18–19, 33 and sch.; DPDP Rules, *supra* note 3.
[74] Ministry of Electronics and Information Technology, *Draft Digital Personal Data Protection Rules, 2025* (3 Jan. 2025).
[75] DPDP Rules, *supra* note 3; DPDP Act, *supra* note 3, s. 18.
[76] DPDP Rules, *supra* note 3, r. 1(2).
[77] Compiled from *Srikrishna Committee Report*, *supra* note 58; DPDP Act, *supra* note 3; DPDP Rules, *supra* note 3.
[78] DPDP Rules, *supra* note 3, r. 1(2).

yet in full force and effect to trigger real disputes, but it's not quite yet finished either, and so courts and litigants are still busy challenging its current contours.

6. Personal Autonomy and Informational Self-Determination: A Conceptual Analysis

The post-Puttaswamy jurisprudence uses the term "personal autonomy" which is best understood as an umbrella term for three analytically distinct, but overlapping, constitutional interests.[79] The first is bodily or physical independence, which is control over one's own body. It is decisional autonomy, the right of a person to make personal relationships decisions without the interference of the state, which is exemplified by Navtej Singh Johar and Joseph Shine.[80] The third and the newest is informational autonomy, otherwise known as informational self-determination: the individual's claim to control the collection, processing and further use of information about herself, even if she has not relinquished any physical possession of that information and even if she originally consented to the collection of that information for a limited purpose.[81]

This is the third strand that the DPDP Act is mainly focused on operationalisation of and where the difference between constitutional theory and statutory design is most apparent. As stated by Puttaswamy, informational self-determination assumes the existence of a data principal who can grant — and no less than refuse — consent with a level playing field with the data fiduciary that is asking for it.[82] The definition of ‘consent' in the DPDP Act, in Section 6, closely models this ideal: consent must be free, specific, informed, unconditional and unambiguous, and can be withdrawn ‘without more difficulty than consenting'.[83] However, in practice, most of the data processing that has a direct impact on the lives of ordinary citizens would not take place under this consent regime at all, but rather under Section 7's "certain legitimate uses" — some of which allow the State to process personal data without requiring any consent at all for the purpose of providing benefits, subsidies, licences and permits.[84] In contexts in which consent is still required, however (like those of the APAAR scheme discussed in Part VII)[85], the structural inequity between an individual (often a child, through a parent, or a citizen who relies upon a government service) and the State puts pressure on the "free" and "unconditional" aspects the Act requires of consent.

The common thread in all three strands, bodily, decisional and informational is the concept of dignity which is constantly mentioned throughout the opinions of Puttaswamy as the value from which autonomy is derived.[86] Dignity, on this reading, is not simply not to be coerced; it also has to be that the person has a meaningful amount of control over decisions and information that are part of her sense of self. This perspective has two implications for the analysis in the following pages. It implies that if the use of consent is merely formalistic — check box, form, notification of exemption — and the person who is targeted by the transaction has no real ability to say no, this alone is not sufficient to satisfy

[79] *Puttaswamy*, *supra* note 1.
[80] *Navtej Singh Johar*, *supra* note 53; *Joseph Shine*, *supra* note 55.
[81] *Puttaswamy*, *supra* note 1 (opinion of Chandrachud, J.).
[82] *Puttaswamy*, *supra* note 1.
[83] DPDP Act, *supra* note 3, s. 6(1), (4).
[84] DPDP Act, *supra* note 3, s. 7(b).
[85] *Abhishek Baxi*, *supra* note 5; *see infra* Part VII(D).
[86] *Puttaswamy*, *supra* note 1 (opinion of Chandrachud, J.).

Article 21.[87] Second, it provides an explanation as to why Indian courts, when faced with disputes that the text of the DPDP Act doesn't tackle head-on, have tended to go beyond it to Puttaswamy's requirement of proportionality and safeguards in the procedures, treating the Act as one of many examples of a constitutional guarantee rather than one that is exclusive.[88]

7. Emerging Constitutional Challenges

This paper looks at seven specific locations of constitutional contest that have developed since the commencement of the DPDP framework in November 2025,[89] each dealing with a different aspect of the Puttaswamy synthesis in the face of the practical requirements of governance, commerce and the digital economy.

A. Executive Exemptions and the Proportionality Deficit

The longest-running constitutional debate is over the exemption from the majority of substantive requirements in the DPDP Act for certain government processing in Section 17.[90] Section 17(1)(c) provides for exemption, on the grounds of research, archiving or statistical activity, while the Central Government, by notification, may exempt on grounds of "sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order or the prevention of incitement to a cognisable offence in relation to any of these grounds" pursuant to Section 17(2).[91] Whereas other comparable exemption clauses, such as in other jurisdictions, include a statement of reasons for the exemption that must be independently agreed upon, reviewed or have a sunset clause, section 17 does not require this.[92]

What this design does not fit well with is Kaul, J.'s demand of "procedural safeguards" against "abuse" of the interference with privacy,[93] a demand that petitioners have raised with the Supreme Court in the consolidated constitutional challenge to the DPDP Act and Rules discussed in sub-part (B) of the associated essay.[94] Whether legitimate or not, an exemption power which can be exercised by the same executive that is being exempted, without any independent ex ante or ex post check, cannot meet the test of ‘legitimate state aim' and proportionality as Puttaswamy interpreted it.[95] In response, the Union government has cited the coverage of these national security exemptions in other national data protection regimes, such as the Personal Data Protection Act of Singapore and the Data Protection Act, 2018 of the United Kingdom,[96] as being typical and not unusual features of data protection law.

---

[87] *Maneka Gandhi*, *supra* note 29 (procedure under Article 21 must be fair, just and reasonable).

[88] *See infra* Part VII.

[89] DPDP Rules, *supra* note 3, r. 1(2).

[90] DPDP Act, *supra* note 3, s. 17.

[91] *Ibid.*, s. 17(2)(a).

[92] DPDP Act, *supra* note 3, s. 17.

[93] *Puttaswamy*, *supra* note 1 (opinion of Kaul, J.).

[94] *The Reporters' Collective Trust v. Union of India*, W.P.(C) No. 211 of 2026, with connected matters (including W.P.(C) Nos. 212, 275, 286, 447 and 722 of 2026), Supreme Court of India (notice issued 16 Feb. 2026) (pending) [hereinafter *DPDP Challenge*]; *see infra* Part VII(B).

[95] *Puttaswamy*, *supra* note 1.

[96] The Personal Data Protection Act 2012 (Act 26 of 2012) (Singapore), s. 4(1)(c); The Data Protection Act, 2018, c. 12, ss. 26–28 (United Kingdom).

B. Privacy versus the Right to Information: Section 44(3)

The second closely related flashpoint relates to Section 44(3) of the DPDP Act, which modifies Section 8(1)(j) of the Right to Information (RTI) Act, 2005.[97] In the past, Section 8(1)(j) provided an exception to disclosure of personal information, which the Supreme Court had, over the last two decades, recognised as part of the freedom of speech and expression under Article 19(1)(a),[98] in favour of public interest that disclosure would serve a greater public interest than disclosure was denied — a proviso that had allowed disclosure of information, including the assets of public officials and the running of welfare schemes, in the State of Uttar Pradesh v. Raj Narain[99] and S.P. Gupta v. Union of India,[100] respectively. This public-interest proviso is omitted from Section 44(3), giving petitioners what they call a blanket exemption for "personal information" from disclosure under the RTI, irrespective of whether the public interest is before the court.[101]

Section 44(3) of the DPDP Act and the rules of the DPDP Rules, 2022, have been a focus of several writ petitions in the Supreme Court,[102] filed by the Reporters' Collective Trust, the National Campaign for People's Right to Information, journalists Geeta Seshu and Anjali Bharadwaj, the Foundation for Media Professionals, DigiPub News India Foundation and Digital News Publishers Association (represented by the Internet Freedom Foundation).[103] The Supreme Court issued notice on the consolidated petitions on 16 February 2026, refused to place a stay on the DPDP framework till the matter was finally considered and remanded the core constitutional issues before a bench of three judges comprising the Chief Justice of India. The bench, presided by the Chief Justice of India, heard the matter again on 27 October 2026,[104] while examining whether the RTI Act and the DPDP Act, both key legislations dealing with personal information, can co-exist or one has to supersede the other. At the time of writing, the issue is still being considered by the court, and it remains to be seen whether Section 44(3) will remain in force under Article 19(1)(a) and Article 21.[105]

C. Independence of the Data Protection Board

Another structural critique is in relation to the Data Security Board of India. The funding, tenure and removal of the Members and the Chairperson of the Board are heavily under executive control,[106] the composition of the search-cum-selection committee that recommends the Members and the Chairperson to the Central Government is also dominated by Government members, and the DPDP Act, 2025, does not prescribe any terms of appointment for the Members. The Telecom Disputes Settlement and Appellate Tribunal is the forum where appeals against the direction of the Board are filed, not the High

[97] DPDP Act, *supra* note 3, s. 44(3); RTI Act, *supra* note 4, s. 8(1)(j).

[98] The Constitution of India, 1950, art. 19(1)(a).

[99] *State of Uttar Pradesh v. Raj Narain*, (1975) 4 SCC 428 : AIR 1975 SC 865.

[100] *S.P. Gupta v. Union of India*, 1981 Supp SCC 87 : AIR 1982 SC 149.

[101] DPDP Act, *supra* note 3, s. 44(3) (amending RTI Act, *supra* note 4, s. 8(1)(j)).

[102] *DPDP Challenge*, *supra* note 94.

[103] Internet Freedom Foundation, "Supreme Court Issues Notice on Constitutional Challenge to the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025" (16 Feb. 2026).

[104] Supreme Court Observer, "Constitutionality of the Digital Personal Data Protection Act, 2023" (Case Page, 2026).

[105] The Constitution of India, 1950, arts. 19(1)(a), 21.

[106] DPDP Act, *supra* note 3, ss. 18–21.

Courts as per provision of Section 29.[107] Petitioners in the pending Supreme Court challenge contend that this design is not representative of the institutional independence that usually attaches to the adjudicatory functions of a tribunal, as in the line of cases that the Madras Bar Association advanced before the Supreme Court,[108] and further contend that an executive-dominated Board will not be able to "serve as an effective executive brake on the executive's own exemptions under Section 17"[109] which is the proportionality shortfall that the Court has identified in sub-part (A).[110] Generally, the government argues that the Board operates in a specialised regulatory capacity, rather than an adjudicatory capacity, and thus does not have the same constitutional obligations.[111]

D. Children's Informational Autonomy: The APAAR Litigation

The most recent example of the Supreme Court directly applying the Puttaswamy principles to an administrative scheme, without relying on the text of the DPDP Act, is the Supreme Court's order in Abhishek Baxi & Ors. v. Union of India & Ors.[112] CBSE schools are required to generate the Aadhaar-linked Automated Permanent Academic Account Registry (APAAR) for their children, which has been challenged by the parents of students attending CBSE affiliated schools before the Supreme Court under Article 32,[113] claiming the consent process followed by the school did not give them the right to refuse and could lead to a lifelong biometric tracking of their children from the early years of school. In both the cases, petitioners relied on the Puttaswamy I proportionality test[114] and also the specific holding in the Aadhaar judgment that children can't be compelled to enrol in Aadhaar without getting their parent/guardian's informed consent.[115]

However, a bench presided over by the Chief Justice of India did not consider the APAAR scheme per se as unconstitutional or agree with the petitioners' request to scrap the scheme in its order dated 20 July 2026.[116] In place of the earlier guidance by the Orissa High Court in Rohit Anand Das v. State of Odisha[117] that parents guardians should be made aware of the presence of a specific rejection clause in the APAAR consent form in that State, Supreme Court had directed the same to be done on a pan-India basis: The model consent form must explicitly include an option to refuse or withhold consent and data collected must not be shared with any private or third party entity unless authorised by law.[118] Importantly the Court has also held that APAAR, even if not established by law but by an executive

[107] DPDP Act, *supra* note 3, ss. 2(a), 29; The Telecom Regulatory Authority of India Act, 1997 (Act 24 of 1997), s. 14.
[108] *See, e.g., Madras Bar Association v. Union of India*, (2014) 10 SCC 1.
[109] *DPDP Challenge*, *supra* note 94.
[110] *See supra* Part VII(A).
[111] *DPDP Challenge*, *supra* note 94.
[112] *Abhishek Baxi*, *supra* note 5.
[113] The Constitution of India, 1950, art. 32.
[114] *Puttaswamy*, *supra* note 1.
[115] *Aadhaar Judgment*, *supra* note 21.
[116] *Abhishek Baxi*, *supra* note 5; *see also* Live Law, "Supreme Court Directs Centre, CBSE to Amend APAAR Consent Form to Give Opt-Out/Refuse Option; Restricts Third-Party Sharing of Data" (25 July 2026).
[117] *Rohit Anand Das v. State of Odisha*, W.P.(C) No. 8285 of 2025, 2025 SCC OnLine Ori 4535.
[118] *Abhishek Baxi*, *supra* note 5.

scheme, will not relieve the authorities implementing it of its duty to comply with the provisions of the DPDP Act.[119]

There are two reasons why the order is instructive. First, it establishes that the requirement of Puttaswamy proportionality and procedural-safeguards is an independent constitutional safeguard over administrative action beyond the express exemptions provided in the DPDP Act — it was not a fault or defect in the Act that the Court was required to identify in order to provide relief. Second, it reveals that there is a structural weakness in the Act's consent system: in the DPDP Act, the model for obtaining consent from children is one of verifiable parental consent,[120] which is really a model of consent from adults transferred to a context where the data subject cannot be part of the consent transaction at all, and which courts would find it harder to provide protections in case-by-case decisions than a more child-specific consent system would have been able to from the beginning.

E. The Right to Be Forgotten and the Open-Justice Tension

In this context, the Delhi High Court's rulings in Laksh Vir Singh Yadav v. Union of India & Ors. and Connected Matters, dated 29 May 2026,[121] in a cluster of over twenty-writ petitions filed during the period from 2016 to 2025, is another instance in which the court has innovatively resolved an issue that the legislature failed to address. The petitioners, including some who had been acquitted from criminal or matrimonial cases or otherwise had no longer been involved in the underlying proceedings, said that the mere fact that their names were linked to judicial proceedings by the search engine, and that their names remained visible in judicial records online years after the proceedings, resulted in continued reputational and dignitary harm without any legitimate public purpose.

The High Court concluded that the right to be forgotten — which it understood to be the right to seek restriction on continued public availability of information about a person that no longer served a legitimate public purpose — was necessarily and naturally flowing from the right to informational privacy which is recognised in Article 21 of Puttaswamy.[122] Concurrently, the Court refused to rule that judicial records need to be deleted in general, but rather devised an alternative remedy of de-indexing name-based searches and masking of personal information – constitutional values that a privacy claim could not be said to abrogate – while allowing the underlying records to remain in official repositories. The Court also held that private, non-state entities like search engines and digital platforms where their functioning violates the Article 21 rights are also subject to writ jurisdiction of the Court[123] and that in proper cases such direction may have an extraterritorial application.

The right to be forgotten of this kind is not expressed in the DPDP Act or Rules. The erasure right provided in Section 12 of the Act[124] applies to the data fiduciary who has the data in question in their possession, but not to an indexing intermediary that does not have an independent relationship to the data principal. The Delhi High Court's order is thus a notable application of Article 21 to the private

[119] DPDP Act, *supra* note 3.

[120] DPDP Act, *supra* note 3, s. 9(1); DPDP Rules, *supra* note 3.

[121] *Laksh Vir Singh Yadav*, *supra* note 6.

[122] *Puttaswamy*, *supra* note 1; *cf.* Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, EU:C:2014:317 (CJEU, 13 May 2014).

[123] The Constitution of India, 1950, art. 226.

[124] DPDP Act, *supra* note 3, s. 12.

digital intermediaries, in the absence of any legislative codification, to the horizontal expansion of an existing constitutional right, which has, for now, been left in the hands of just one High Court.[125]

F. Digital Access as a Precondition for Autonomy

Another, distinct, addition to Article 21 has been seen in Amar Jain v. Union of India, which was filed along with Pragya Prasun v. Union of India,[126] where disability-rights petitioners had contended that the inaccessibility of digital platforms, ranging from government e-governance websites to banking applications and public services, was an infringement of their right to "meaningful participation" in civic and economic life. Justice Srikrishna, in his opinion, read a right to inclusive digital access into the right to life under Article 21, specifically on the basis of dignity and autonomy, as encompassed in Puttaswamy's reasoning,[127] and also on the basis of accessible access under the statutory provisions of the Rights of Persons with Disabilities Act, 2016,[128] as applicable to the situation.

Amar Jain is important for this paper because he indicates that the autonomy provided by the data protection is conceptually tied to a structural guarantee of access. Without access to the digital platform on which a right to consent, correction, or erasure must be exercised, such rights are little more than window-dressing. In addition to the informational strand on self-determination as discussed by Puttaswamy, Amar Jain suggests that there are two complementary axes to constitutional protection of personal autonomy in the digital world: control over one's data, once inside the digital world and the ability to enter the digital world on an equal footing at all.[129]

G. Algorithmic Decision-Making: An Unaddressed Frontier

Last but not least, the current framework does not address at all one key aspect of informational autonomy: automated and algorithmic decision-making. While the EU's General Data Protection Regulation (GDPR) also stipulates a qualified right not to be subject to a decision based exclusively on automated processing,[130] the DPDP Act does not include a corresponding directive for algorithmic credit-scoring, welfare eligibility assessment or content moderation, among others, processes which are increasingly shaping citizens' access to state and market services. This is an important omission because other Indian regulators are already starting to tackle the very "black-box" accountability issue in related areas, such as the Securities and Exchange Board of India's new guidelines for retail investors to participate in algorithmic trading, which require exchange approval for proprietary trading algorithms, a unique identifier, and even, in the case of undisclosed "black-box" algorithms, registration of the provider as a research analyst.[131] The DPDP Act does not currently provide a similar mechanism of accountability with regard to the algorithmic processing of personal data, and the need to explain and contest the processing of personal data is something that can only be addressed, if at all, through future

[125] *Laksh Vir Singh Yadav*, *supra* note 6.
[126] *Amar Jain*, *supra* note 7.
[127] *Puttaswamy*, *supra* note 1.
[128] The Rights of Persons with Disabilities Act, 2016 (Act 49 of 2016), ss. 40, 42.
[129] *Amar Jain*, *supra* note 7; *Puttaswamy*, *supra* note 1.
[130] GDPR, *supra* note 60, art. 22.
[131] Securities and Exchange Board of India, Circular on "Safer participation of retail investors in Algorithmic trading" (4 Feb. 2025); *see also* The Securities and Exchange Board of India (Research Analysts) Regulations, 2014.

amendments and further judicial interpretation of the nature of the algorithmic processing of personal data as has been seen in sub-parts (D) and (E) above.[132]

8. Critical Analysis: Balancing State, Market and Individual Autonomy

The conflicts discussed in Part VII illustrate unevenness in constitutional enforcement. In cases where the controversy is around a recognisable administrative scheme (APAAR)[133] or an identifiable category of private actors (search engines and digital platforms),[134] courts have demonstrated not only a willingness to apply the Puttaswamy principle on proportionality and procedural safeguards directly, but also practically, by designing specific remedies within months of the petitions being filed. But where the dispute is with the exemption architecture of the DPDP Act, Section 17's government exemptions, Section 44(3)'s amendment of the RTI Act, and the composition of the Data Protection Board, the same courts have taken a much more measured, and cautious, approach, granting notice, refusing interim relief, and sending matters to larger benches[135] — and none of the cases have been resolved more than a year after the first petitions were filed and nearly nine years after Puttaswamy itself.[136]

This asymmetry is quite easily understood structurally. Challenges to an executive scheme or to a private platform's practices allow a court to employ a well-established constitutional test to a clearly delineated fact pattern, and to provide a remedy that does not invalidate the scheme's statutory or regulatory structure. A challenge to Parliament's own legislative decisions — especially decisions which have been arrived at after a rather protracted, contentious legislative history, and were made with deliberate thought — beggars a court to deal directly with the issue of separation of powers, and Indian courts have never been comfortable in directly engaging with the issue of separation of powers,[137] preferring to take incremental steps in the way of notice and hearing rather than granting summary interim relief.[138] The net outcome is a double-sided jurisprudence, one of quick, substantive enforcement of autonomy against an identifiable administrative and private actor, and the other of slow, procedural, and cautious engagement with the very statute that was enacted to vindicate autonomy.

The pattern evinces a normative lesson for the next wave of Indian data protection jurisprudence, a lesson not one that scholarship could speak to without the benefit of natural experience of the law currently in operation, as the DPDP Act.[139] The Puttaswamy framework has proven useful in the context of specific, factually limited claims to autonomy,[140] but is unlikely to be decisive in the outcome of the Supreme Court case, though it will undoubtedly have a great deal to do with how the Court determines to rule in the future on the architecture of the data protection statute itself. In the literal sense, until that challenge is met the exact nature of personal autonomy under Article 21 is yet to be determined, when the State acts in its own interest, as opposed to the interest of a third-party administrator or platform.[141]

---

[132] *See supra* Part VII(D)–(E).

[133] *Abhishek Baxi*, *supra* note 5.

[134] *Laksh Vir Singh Yadav*, *supra* note 6.

[135] *DPDP Challenge*, *supra* note 94.

[136] *Puttaswamy*, *supra* note 1.

[137] *See, e.g.*, *Kesavananda Bharati v. State of Kerala*, (1973) 4 SCC 225 : AIR 1973 SC 1461.

[138] *See Ram Krishna Dalmia v. Justice S.R. Tendolkar*, AIR 1958 SC 538 (presumption of constitutionality of legislation).

[139] DPDP Act, *supra* note 3.

[140] *Puttaswamy*, *supra* note 1; *Abhishek Baxi*, *supra* note 5; *Laksh Vir Singh Yadav*, *supra* note 6.

[141] *See supra* Part VII(A)–(E).

9. Conclusion and Future Scope

This paper has suggested that, since Puttaswamy, the strand of Indian constitutional law that pertains to data protection and personal autonomy has shifted from a declaratory stage – that privacy and autonomy are guaranteed by Article 21 in all circumstances – to a stage of implementation where each clause of Article 21 is negotiated with the specific statutory structure of the Digital Personal Data Protection Act, 2023. The historical sections of this paper sketched the long and winding path from the narrow readings of M.P. Sharma and Kharak Singh,[142] through Maneka Gandhi's golden triangle[143] to a disjointed line of context-specific privacy cases and onto the authoritative synthesis of Puttaswamy;[144] the legislative sections traced the six-year, slow-moving path from the Srikrishna Committee's report to the November 2025 coming into force of the DPDP Act;[145] and Part VII analysis showed how that synthesis is now being litigated in constitutional conflicts involving executive exemptions, access to information, regulatory independence, children's data, the right to be forgotten, and digital access in general.[146]

As of this writing, several questions remain genuinely open, and make a natural agenda for future research. The meaning of the word's "proportionality" and "procedural safeguards" will likely become the most significant limitation on the state's own exceptions to data processing under the DPDP Act, if the challenge to the Act succeeds.[147] The challenges to the consent provisions in the DPDP Act raised in the APAAR case,[148] though not resolved, point to the need for a specific legislative solution to this issue, rather than ad hoc judicial tinkering. In the absence of any legislative codification, or appellate clarification, the Delhi High Court's right-to-be-forgotten decision in Article 21 could be difficult to implement beyond its blanket jurisdiction.[149] Without any policy or law addressing algorithmic decision-making, what is sure to be the next great topic in personal autonomy law remains unanswered.[150] In other words, India's data protection law is just beginning, its constitutional significance is still in the process of being drafted.

References

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. K.S. Puttaswamy v. Union of India (Aadhaar), (2019) 1 SCC 1.
3. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
4. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
5. A.K. Gopalan v. State of Madras, AIR 1950 SC 27.
6. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
7. Govind v. State of Madhya Pradesh, (1975) 2 SCC 148.
8. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
9. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

[142] *M.P. Sharma*, *supra* note 24; *Kharak Singh*, *supra* note 2.
[143] *Maneka Gandhi*, *supra* note 29.
[144] *Puttaswamy*, *supra* note 1.
[145] DPDP Act, *supra* note 3; DPDP Rules, *supra* note 3.
[146] *See supra* Part VII(A)–(F).
[147] *DPDP Challenge*, *supra* note 94.
[148] *Abhishek Baxi*, *supra* note 5.
[149] *Laksh Vir Singh Yadav*, *supra* note 6.
[150] *See supra* Part VII(G).

10. Navtej Singh Johar v. Union of India, (2018) 10 SCC 1.
11. Joseph Shine v. Union of India, (2019) 3 SCC 39.
12. State of Uttar Pradesh v. Raj Narain, (1975) 4 SCC 428.
13. S.P. Gupta v. Union of India, 1981 Supp SCC 87.
14. Amar Jain v. Union of India; Pragya Prasun v. Union of India, W.P.(C) No. 49 of 2025 & W.P.(C) No. 289 of 2024, Supreme Court of India, decided 30 April 2025.
15. Abhishek Baxi & Ors. v. Union of India & Ors., W.P.(C) No. 832 of 2026, 2026 SCC OnLine SC 1391, decided 20 July 2026.
16. Rohit Anand Das v. State of Odisha, W.P.(C) No. 8285 of 2025, 2025 SCC OnLine Ori 4535.
17. Laksh Vir Singh Yadav v. Union of India & Ors. and Connected Matters, W.P.(C) 1021/2016 & Connected Matters, Delhi High Court, Neutral Citation 2026:DHC:4891, decided 29 May 2026.
18. Constitutionality of the Digital Personal Data Protection Act, 2023 (consolidated matters including The Reporters' Collective Trust v. Union of India, W.P.(C) 211/2026; National Campaign for People's Right to Information v. Union of India, W.P.(C) 212/2026; Geeta Seshu v. Union of India, W.P.(C) 275/2026; Anjali Bharadwaj v. Union of India, W.P.(C) 286/2026; Foundation for Media Professionals & Anr. v. Union of India, W.P.(C) 447/2026; DigiPub India News Foundation v. Union of India, W.P.(C) 722/2026; Digital News Publishers Association v. Union of India), Supreme Court of India, notice issued 16 February 2026, pending.
19. The Constitution of India, 1950, art. 21.
20. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
21. The Digital Personal Data Protection Rules, 2025, notified 13–14 November 2025.
22. The Right to Information Act, 2005.
23. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
24. The Rights of Persons with Disabilities Act, 2016.
25. Committee of Experts on Data Protection (Chair: Justice B.N. Srikrishna), *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, July 2018).
26. PRS Legislative Research, "Digital Personal Data Protection Bill, 2023" (Bill Summary, 2023).
27. Internet Freedom Foundation, "Supreme Court Issues Notice on Constitutional Challenge to the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025" (16 February 2026).
28. Supreme Court Observer, "Constitutionality of the Digital Personal Data Protection Act, 2023" (Case Page, 2026).
29. Live Law, "Supreme Court Directs Centre, CBSE to Amend APAAR Consent Form to Give Opt-Out/Refuse Option; Restricts Third-Party Sharing of Data" (25 July 2026).
30. Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules 2025 — Gazette Notification, G.S.R. 846(E) (13 November 2025).