International Journal of
Law, Politics and Governance
ISSN: 3143-7028 | https://www.ioro.org/ijlpg

Digital Governance and Constitutional Rights in India: Reconciling Administrative Efficiency with Privacy, Equality and Due Process

Dr Tangutur Aparna [1,*]

[1] *Department of Law, Osmania University, Hyderabad, Telangana, India*

* **Corresponding author:** aparnat.law@gmail.com

Abstract

India's shift towards digitally mediated governance has reshaped the citizen-administrative state dynamics. Biometric identity framework (Aadhaar), faceless assessment in the income tax administration, direct benefit transfer system and the Digital Personal Data Protection Act, 2023 are expected to be efficient, leak-proof and targeted, but leave questions unanswered before the court. This article questions whether the digital governance ecosystem in India has sufficiently harmonized the efficiency of administration with the fundamental rights of privacy, equality of substantive rights, and procedural rights in Article 21, 14 and due process. The article uses the doctrinal approach to examine the jurisprudence of the Supreme Court of India on 'informational privacy' and 'proportionality', as well as the statutory framework of the Aadhaar Act, 2016, the Information Technology Act, 2000, and Digital Personal Data Protection Act, 2023; and the administrative practice of algorithmic and automated decision-making in welfare and taxation. It believes that the judiciary has created a functional test of proportionality for privacy interests, but this test continues to be under-respected when it comes to algorithmic exclusion and automated adjudication, where reasoned decision making and meaningful review are often lacking. The article then envisions a calibrated approach that combines proportionality review with a compulsory duty of explaining algorithms and a system of independent institutional oversight, ensuring that enhanced efficiency in government does not sacrifice constitutionally protected rights.

Keywords: digital governance; right to privacy; Aadhaar; algorithmic discrimination; due process; Digital Personal Data Protection Act, 2023; administrative law

1. Introduction

India is the home of one of the world's most diverse and large population bases and has been in a unique process of digitisation of governance over the past 10 years. More than 1.3 billion people are now registered in the Aadhaar programme and the DBT system now distributes subsidies for food, cooking gas, pensions and scholarships through Aadhaar-linked bank accounts; the income tax assessments are increasingly faceless and automated; and, for the first time, India has a general statute on the processing of personal data, namely the Digital Personal Data Protection Act, 2023 ("DPDP Act"). They are often described in terms of efficiency, that is, leakages of subsidy are minimised, services are delivered faster, transaction costs are reduced, and the interface between the citizen and the State is paperless. But each of these devices functions on constitutional space that was just recently charted by the Supreme Court of India. In Justice K.S. Puttaswamy (Retd.) v. Union of India[1], the nine-judge Bench unanimously found that the right to privacy is implicit in the right to life and personal liberty under Article 21 and also exists under Articles 14 and 19 of the Constitution. The judgment not only acknowledged a right, but it also laid the groundwork for the constitutionality of the way in which the state can lawfully limit that right, and established a strict proportionality test that must have a rational connection between means and ends, necessity and a legitimate state end, and legality. This test was adopted in the subsequent five-judge Aadhaar judgment, Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.)[2], where it upheld the Aadhaar Act, 2016 in a modified form and invalidated provisions allowing private use of Aadhaar authentication under the old Section 57.

This article questions whether the proportionality doctrine that has grown out of these two judgments, in conjunction with the safeguards contained in the DPDP Act, 2023 and administrative law in general, is sufficient to tackle the challenges that India's burgeoning digital governance framework places on it. It claims that the framework is more appropriate for resolving ad hoc privacy disputes, but structurally weaker when the harm is from algorithmic debarment from welfare or automated administrative decision-making with no reason to challenge. The goal is therefore to sketch the Indian constitutional and statutory framework of digital governance on the three fronts of privacy, equality and due process and highlight specific gaps in that framework where citizens' rights to privacy and equality and due process are being compromised, suggesting a calibrated reform.

2. Literature Review

Scholarship on digital governance in India has developed along three broadly separate strands, which this review draws together because the doctrinal analysis in this article treats them as facets of a single constitutional problem rather than as independent silos.

2.1. Privacy, Proportionality and Informational Self-Determination

The first one interacts with the doctrinal structure of the Right to Privacy. Much of this literature has been on the nature of the proportionality test itself, especially whether the courts in India are as rigorous with the fourth limb of legality, legitimate aim and necessity, as they are with the first three limbs, that is, whether they include a genuine balancing of the benefits of the measure against its costs to the right holder. The idea of "informational self-determination", which is borrowed from German constitutional law, is another aspect that has been discussed by commentators, and that does not sit well with an Aadhaar architecture which involves centralised storage of biometric information instead of minimisation at the point of authentication.

2.2. Equality, Exclusion and the Digital Divide

A second strand, more empirical, has highlighted cases in which exclusion from public distribution and pension schemes resulted from the failure of biometric authentication, because the fingerprints of the elderly, manual-labouring or disabled residents were unreadable, or due to the lack of network connectivity in rural areas which made real-time authentication impossible. This literature begins by placing such exclusion in the context of the Article 14 doctrine of manifest arbitrariness, as enunciated in E.P. Royappa v. State of Tamil Nadu[3], and reinforced by Maneka Gandhi v. Union of India[4], that a facially neutral

[1] Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2017) 10 SCC 1.

[2] Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.), (2019) 1 SCC 1.

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

[4] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

authentication requirement can produce substantively unequal outcomes for groups least equipped to navigate digital infrastructure.

2.3. Due Process and Automated Administrative Decision-Making

The third strand is based on the principles of administrative law, and deals with the consistency of automated decision-making or algorithmically assisted decision-making, such as in the faceless assessment scheme under the Income-tax Act, 1961, and in Aadhaar-based authentication failures without any justification resulting in the denial of benefits. This literature asks whether the same degree of transparency is expected in a situation where the proximate cause of a rights-restricting outcome is an algorithm, instead of an executive order, as in Anuradha Bhasin. It asks whether the same level of transparency should apply to an algorithm, as opposed to an executive order, that is the proximate cause of a rights-restricting outcome, as in Anuradha Bhasin v. Union of India[5].

Together, this collection of cases demonstrates that privacy, equality and due process are not distinct spheres in the digital governance context; loss of access to a subsidy due to authentication failure is a privacy loss (compulsory biometric disclosure), an equality loss (disparate impact on the digitally marginalised) and a due process loss (lack of a reasoned, reviewable decision). The lacuna this article highlights is the comparative under-theorisation and under-litigation of the equality and due process dimensions of Indian doctrine.

3. Methodology

The doctrinal legal research and comparative constitutional analysis method is used in this article. Primary sources include the text of the Constitution of India[6], the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016[7], the Information Technology Act, 2000[8], and the Digital Personal Data Protection Act, 2023[9], as well as the judgments of the Supreme Court of India referred to above, when read with relevant High Court judgments that shed light on the working of these acts at the point of application. The doctrinal analysis is carried out in three steps. First, the proportionality standard laid down in Puttaswamy (Privacy-9J.) and followed in Puttaswamy (Aadhaar-5J.) is extracted from the judgments, taking into account the four limbs which the plurality opinion in Puttaswamy (Aadhaar-5J.) highlighted. Secondly, a provision-by-provision analysis of the statutory provisions of the Aadhaar Act, Information Technology Act and DPDP Act is conducted, and the safeguards and exemptions provided in each are discussed, with special focus on state use exemptions that can weaken the proportionality requirement in implementation. Third, material from the secondary sources, such as reports by the parliamentary standing committees, government responses to the Right to Information Act, 2005, and documented instances of authentication failure reported by civil society organisations[10], is used to verify whether the doctrinal safeguards are effective when schemes are scaled up. This triangulation between constitutional construction, the words of the statute and implementation evidence is supposed to serve as a measure to test not only what the law says, but what it does.

[5] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

[6] The Constitution of India, 1950, arts. 14, 19, 21.

[7] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, India Code.

[8] Information Technology Act, No. 21 of 2000, India Code (as amended by the Information Technology (Amendment) Act, No. 10 of 2009).

[9] Digital Personal Data Protection Act, No. 22 of 2023, India Code.

[10] Ministry of Electronics and Information Technology, Government of India, Report of the Committee of Experts on a Data Protection Framework for India, 2018; Standing Committee on Finance, Lok Sabha, Report on the Digital Personal Data Protection Bill, 2022, Parliament of India, 2023 (cited infra note 15); R. Khera, "Impact of Aadhaar on Welfare Programmes," 52(50) Econ. Polit. Wkly. 61, 61–70 (2017).

4. Analysis: Privacy, Equality and Due Process in India's Digital Governance Architecture

4.1. Privacy and the Proportionality Standard

Based on Puttaswamy (privacy 9J.), the proportionality standard, any state action limiting privacy must, among other things, meet the test of being proportionate, meaning it must be: (i) authorized by law, (ii) directed toward a legitimate aim, and (iii) necessary, meaning it cannot be achieved through a less intrusive means. It must also be proportionate in the sense of maintaining a fair balance of rights and interests. Together, the four limbs of this proportionality test are measured against the facts of the Aadhaar case in Puttaswamy (Aadhaar 5J.). Here the majority constitutional bench determined that the essential system of the Aadhaar scheme, compulsory biometric data collection to claim certain government benefits under Section 7 of the Aadhaar Act[11] met the test of a legitimate aim, leaving specified proportionate, as the safeguards within the scheme, like data minimization and limitation on the usage of authentication records, optimized the scheme's coexistence with an individual's right to privacy, compliance with the law and any legitimate aim.

Meanwhile, the majority also struck down the old Section 57 of the Aadhaar Act[12] that had authorized private corporate bodies to enforce Aadhaar-authentication as a pre-condition to service, holding that this contravention into the private sphere was at best unnecessary for the scheme's welfare-delivery goal that justified such a scheme originally, and at worse, a harbinger of profiling, by aggregating authentication traffic of otherwise unrelated private services. The restriction of the use of Aadhaar[13] by the state for welfare delivery, and that by private bodies for commercial convenience, is the doctrinal anchor for the proportionality analysis that later shaped draft regulation of the DPDP Act, 2023.[14] The 2023 DPDP Act codifies several aspects of this precedent: it prohibits the processing of personal data unless a not duty-bound "lawful purpose" is pursued, and the processing is either based on the consent of the data principal or explicit statutory "legitimate use" ground; and it establishes a Data Protection Board with limited powers to inquire into complaints and impose financial sanctions.

But whereas the '22 PDP Bill explicitly incorporates Puttaswamy 's four-part proportionality test into part 2 legitimate use exception, the ongoing legislative process introduces significant reservations to the core jurisprudence by providing for notable exemptions for state/instrumental processing and non-personal data processing/processing of aggregations in the interests of sovereignty, security, public order and prevention of offences without explicitly including the four-part test in the statutory exemption. Due to the framing of this exclusion by reference to the purpose invoked (rather than necessity/balance), its substantive scope is very likely to turn on how narrowly courts construe state interests' denoting 'in the interests of' the listed and empowered grounds, which the Supreme Court has not yet addressed as to the 2023 Act.

4.2. Equality and Algorithmic Exclusion

The equality strand of digital governance in India has manifested itself most clearly in the exclusions from the Public Distribution System and social security pensions, as recorded. In practice, as a consequence of the above, authentication failure constituted a denial of the underlying right, even though it was not explicitly mentioned as a cause of denial of benefit in the Aadhaar Act or the relevant welfare legislation, given that a very large population, like elderly persons, manual labourers and persons with certain disabilities, has fingers

[11] Aadhaar Act, 2016, supra note 8, § 7.

[12] Aadhaar Act, 2016, supra note 8, § 57 (since struck down in Puttaswamy (Aadhaar-5J.), supra note 2).

[13] Puttaswamy (Aadhaar-5J.), supra note 2, at para. 269.

[14] Standing Committee on Finance, Lok Sabha, Report on the Digital Personal Data Protection Bill, 2022, Parliament of India, 2023.

which do not match the biometric template on record. This discrepancy between the letter of the entitlement and the algorithmic delivery of the entitlement, which is an indirect kind of inequality, technologically produced, is exactly the type of inequality that the classical Article 14, arbitrariness doctrine cannot foresee.

In Maneka Gandhi v. Union of India[15] it had been held that the procedure for the deprivation of a right guaranteed by Article 21 must be fair, just and reasonable and not just in form prescribed by law. The principle has been applied to the authentication failure situation to argue that a welfare scheme must not be able to require a person, even if the person is unwilling and unable to produce a biometric match, to provide a welfare benefit as a condition of the subsistence entitlement, without offering an accessible and effective alternative verification pathway. This concern is also reflected in the Aadhaar Act, which states in Section 7[16] that in cases where verification using Aadhaar is not possible, verification on alternative documents shall be allowed, and time and again circulars have been issued by the Ministry that no beneficiary shall be denied any entitlement for failure to obtain Aadhaar. The fact that this formal safeguard is not working in practice suggests that there is a substantive, rather than a purely textual, issue: the other route is rarely made use of at the point of delivery, and the one who is deprived of a subsidy does not have a forum to challenge the subsidy's denial in real time.

A similar equality issue is raised by the digital divide. The assumption of direct benefit transfer, faceless assessment, and e-governance portals is that people are digitally literate, have access to smartphones, and are connected to the internet, all of which are distributed unevenly by gender, caste, class, and geography. When, in the guise of a formally neutral redesign, a scheme is implemented using a digital-first interface without an adequate offline or assisted-access option, it is a substantially regressive measure, and the rationale for this was exactly the one proposed by E.P. Royappa and its followers[17], though this issue has not been argued to this extent in those terms.

Table 1. Comparative snapshot of India's principal digital governance statutes.

Statute	Primary Objective	Key Safeguard / Residual Gap
Aadhaar Act, 2016	Unique biometric identity for targeted delivery of subsidies, benefits and services	Section 7 permits alternative identification, but implementation at the point of delivery is inconsistent
Information Technology Act, 2000 (as amended 2008)	Legal recognition of electronic records and cybercrime regulation	Section 43A imposes liability for data breaches by body corporates, but has no equivalent obligation on government bodies
Digital Personal Data Protection Act, 2023	General regime for processing of digital personal data and grievance redress through a Data Protection Board	Section 17 state-use exemptions are not expressly conditioned on the Puttaswamy proportionality test

4.3. Due Process and Automated Administrative Decision-Making

The third axis relates to the compatibility of automatic and algorithmically supported decision-making with the guarantees of due process embedded in Art. 21 and other rules of natural justice which regulate

[15] Maneka Gandhi v. Union of India, supra note 5.

[16] Aadhaar Act, 2016, supra note 8, § 7.

[17] E.P. Royappa, supra note 4.

administrative action. The faceless assessment scheme introduced in the Income-tax Act, 1961 eliminates the direct interaction between the assessing officer and taxpayer; it would go through a centralised and technology-enabled interface with the purpose of minimising discretion and corruption. The scheme has been litigated on the merits of whether taxpayers had a real opportunity to comment on adverse orders, whether or not such opportunity was shortened by the use of automated systems that left short response periods, or whether the taxpayers' responses were not even counted.

Anuradha Bhasin v. Union of India is a helpful, although analogically flawed, precedent. There, the Court ruled that any executive order that interferes with a fundamental right must be published, have reasons, and be subject to challenge before a review committee, a principle extended to Internet shutdowns but generally to any exercise of state power that impinges on rights. An automated administrative determination in the assessment of tax or delivery of welfare benefits is not an executive order in the sense of Anuradha Bhasin, but it does have the structural characteristic of one or more rights-affecting outcomes being produced by a process that the affected person cannot meaningfully interrogate. The Aadhaar Act or the Income-tax Act does not yet contain a publish and reason requirement similar to what has been established in Anuradha Bhasin, leaving a due process gap at the point where the citizen is least able to see the process, namely, at the time of the decision. This divide is not just theoretical. In most cases where an algorithm does not grant a subsidy, flags a tax return for review or refuses to match a biometric, the person concerned will receive, at best, a code generated by the system, and the appeals or grievances process provided is often as automated and as opaque as the process that originally denied the subsidy. The following considerations recur across the schemes examined in this article:

- Absence of a statutory duty to provide an intelligible, individualised explanation for an adverse automated decision.
- Grievance redress mechanisms that are themselves automated, producing a further layer of unreviewable decision-making rather than independent human oversight.
- Limited institutional capacity within bodies such as the Data Protection Board to audit algorithmic systems proactively, as opposed to responding to individual complaints after harm has occurred.

Combined, the three axes, namely privacy, equality and due process, expose a common structural weakness: the Indian Constitution and statutory framework are fairly well structured to address a discrete privacy claim after an identifiable harm, but are not quite so structured to address the cumulative and diffuse harms that may result from an efficient administration at scale, without individualized reasoning or independent audit.

5. Discussion

The analysis above indicates that while the Puttaswamy proportionality standard, as a doctrinal exercise, was a well-thought-out answer to a narrower question than the one which digital governance is now posing. Proportionality review makes several assumptions, including that a claimant can be identified, a measure can be identified, and a court can consider the costs of a measure in relation to the benefits in a particular case. It is a strong test to determine the constitutionality of a statutory scheme in the abstract, like Aadhaar or a data-processing provision in the DPDP Act. It's a much less effective mechanism for the identification and remedy of the "damaged goods" that result from authentication failure or algorithmic exclusion at the point of implementation (POI), as no single litigant may have the incentive, information, or resources to bring such a lawsuit, and the damage itself may not be limited to a single reviewable decision. The equality and due process aspects of digital governance need to be addressed institutionally, not just through adjudicative processes. Experience in other parts of the world is instructive here, but not directly transferable: the GDPR[18], which was adopted by the EU in 2016, contains a right to an explanation and to human review of automated decisions with legal consequences and a high level of impact. The EU AI Act[19], which was adopted in 2021, also requires ex ante conformity checks on systems that are capable of making “automated decisions with a high degree of impact and which produce legal or similarly significant consequences for them” in essential public services and benefits. The current Indian DPDP Act 2023 does not include a corresponding right to meaningful human review of automated decisions, or a requirement for a pre-deployment audit of high-risk scenarios involving the government, such as welfare assessment using biometric data or automated tax assessment.

Another restriction is the institutional structure of the Data Protection Board provided for by the DPDP Act, 2023. In contrast to proactive sectoral regulators, the Board is not organized primarily as an inspection authority, but a complaint adjudication authority, responding to complaints rather than conducting its own audit of data systems that are considered high risk. In a complaint-driven system, the one-sided information and resources of an individual welfare recipient and the state agency operating the authentication system will not lead to systemic exclusion until it creates extensive damage.

None of this implies that Aadhaar or the DPDP Act ought to be torn up or that they ought to be declared unconstitutional; both are constitutional and valid solutions to real issues of welfare leakage and data governance. The argument is more limited: it is that an explainability and institutional-audit standard that can deal with harms which are structural, not episodic, must be added to the proportionality standard in privacy claims, not displaced. The ideas presented in the next section are woven together into a specific proposal.

6. Conclusion

This article has examined the constitutional architecture governing India's digital governance apparatus across three axes, namely privacy, equality and due process, and has argued that while the Supreme Court's proportionality jurisprudence in *Puttaswamy (Privacy-9J.)* and *Puttaswamy (Aadhaar-5J.)* provides a robust standard for adjudicating discrete privacy claims, it does not, by itself, adequately address the equality and due process harms produced by algorithmic exclusion and automated administrative decision-making at scale.

The article proposes a calibrated framework with three elements. First, the proportionality standard should be read, or legislatively clarified, to apply expressly to the state-use exemptions in Section 17 of the DPDP Act, 2023[20], so that invocation of a listed ground is not treated as self-certifying but remains subject to necessity and balancing scrutiny. Second, Parliament should consider introducing a statutory right to an intelligible explanation and to human review for automated decisions that affect access to welfare entitlements or trigger adverse tax consequences, modelled on but adapted to Indian administrative capacity[21] rather than transplanted wholesale from the GDPR. Third, the Data Protection Board should be empowered and resourced to conduct proactive, risk-based audits of high-risk government data systems, including biometric welfare authentication and automated assessment schemes, rather than functioning solely as a reactive complaint-adjudication forum.

[18] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 22.

[19] Regulation (EU) 2024/1689 (Artificial Intelligence Act), 2024 O.J. (L series).

[20] Digital Personal Data Protection Act, 2023, supra note 10, § 17.

[21] A. Bhatia and G. Bhatia, "The Transformative Constitution and the Right to Privacy," 30(1) Natl. Law Sch. India Rev. 1, 1–25 (2018).

Such changes would not take away the efficiency improvement that Aadhaar and faceless assessment and the DPDP Act brought, but would ensure that this efficiency is achieved without the citizens who are the least able to challenge it bearing the burden of the error. Empirically, it would be interesting to explore the prevalence and distribution of authentication-exclusion in other jurisdictions dealing with similar administrative digitisation, and to compare the design of algorithmic audit mechanisms.

Acknowledgements

The author thanks the Department of Law, Osmania University, for institutional support during the preparation of this article. No individual contributor other than the author is acknowledged.

Funding

This research received no external funding.

Conflict of Interest

The author declares no conflict of interest.

Data Availability Statement

This is a doctrinal legal study and does not involve the generation or analysis of a proprietary dataset. All primary sources relied upon, including the Constitution of India, the Aadhaar Act, 2016, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the judicial decisions cited, are in the public domain and are identified in the References.

AI Usage Disclosure

Generative AI tools like Gemini were used in a very limited capacity for language refinement and formatting assistance during manuscript preparation. All legal analysis, argumentation, citation verification and conclusions are the author's own and have been independently reviewed against primary legal sources.

Author Contributions

Conceptualization, T.A.; methodology, T.A.; formal analysis, T.A.; writing (original draft), T.A.; writing (review and editing), T.A. The author has read and agreed to the published version of the manuscript.

References

[1] Constitution of India, 1950, arts. 14, 19, 21.

[2] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, India Code.

[3] Information Technology Act, No. 21 of 2000, India Code (as amended by the Information Technology (Amendment) Act, No. 10 of 2009).

[4] Digital Personal Data Protection Act, No. 22 of 2023, India Code.

[5] Income-tax Act, No. 43 of 1961, India Code, s. 144B (faceless assessment).

[6] Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2017) 10 SCC 1.

[7] Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.), (2019) 1 SCC 1.

[8] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

[9] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

[10] E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.

[11] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

[12] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

[13] S. Bhandari and R. Sane, "Towards a robust legal identity framework: an analysis of the Aadhaar Act," Indian J. Law Technol., vol. 12, no. 1, pp. 1–30, 2016.

[14] U. Ramanathan, "Considering social implications of biometric registration: a database intended for every resident of India," Comput. Soc. Newsl., ACM SIGCAS, 2010.

[15] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 22.

[16] Regulation (EU) 2024/1689 (Artificial Intelligence Act), 2024 O.J. (L series).

[17] Ministry of Electronics and Information Technology, Government of India, Report of the Committee of Experts on a Data Protection Framework for India, 2018.

[18] Standing Committee on Finance, Lok Sabha, Report on the Digital Personal Data Protection Bill, 2022, Parliament of India, 2023.

[19] R. Khera, "Impact of Aadhaar on welfare programmes," Econ. Polit. Wkly., vol. 52, no. 50, pp. 61–70, 2017.

[20] A. Bhatia and G. Bhatia, "The transformative constitution and the right to privacy," Natl. Law Sch. India Rev., vol. 30, no. 1, pp. 1–25, 2018.

Appendix A. Key Statutes and Case Law Referenced

[21] This appendix consolidates, for ease of reference, the principal legal instruments discussed in this article.

[22] Constitution of India, 1950: Articles 14 (equality before law), 19 (freedom of speech and movement) and 21 (protection of life and personal liberty).

[23] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016: Sections 7 (requirement of Aadhaar for specified subsidies) and the erstwhile Section 57 (struck down in Puttaswamy (Aadhaar-5J.)).

[24] Digital Personal Data Protection Act, 2023: Sections on notice and consent, “legitimate uses,” the Data Protection Board, and Section 17 state-use exemptions.

[25] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 and (2019) 1 SCC 1, the privacy and Aadhaar judgments respectively.

[26] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637, proportionality standard for rights-restricting executive orders.