



INDIA'S DIGITAL IDENTITY REGIME: PRIVACY, SURVEILLANCE, AND CONSTITUTIONAL CHALLENGES

Raagya Vashishtha*

ABSTRACT

India's digital identity regime is critically analysed in this essay, with Aadhaar at its centre, from the perspective of constitutional law, right to privacy, and surveillance regulation. It discusses how biometric identification systems, initially intended for welfare provision and administrative streamlining, have now spread into policing, finance, and telecommunications, creating grave issues with regard to data security and civil rights. Rooted in the historic K.S. Puttaswamy v. Union of India (2017) ruling, where privacy was held to be a fundamental right, the paper analyses whether India's existing legal framework, comprising the Digital Personal Data Protection Act, 2023, is sufficient to protect individual autonomy. It identifies the Act's sweeping exemptions to state agencies, absence of independent regulation, and feeble enforcement provisions, contending that they compromise the proportionality principle and enable unrestricted surveillance. The research also contrasts India's process with global benchmarks like the EU's GDPR, Council of Europe's Convention 108+, and OECD's transparency guidelines and finds a wide disparity in rights-based shields. The phenomenon of "function creep" is discussed to identify ways in which digital ID systems are reassigned for uses beyond their original design, most time without the provision of necessary legal shields. The research concludes by suggesting privacy-by-design principles, more robust judicial and parliamentary scrutiny, and conformity with international human rights frameworks to safeguard constitutional values from being undermined. By situating a substantial examination of legal documents, policy evolution, and comparative mechanisms within the body of research, this work contributes to the ongoing discourse about how digital governance should accommodate efficiency with the safeguard of constitutional rights in a democratic polity.

*BBA LLB (HONS.), SECOND YEAR, VIVEKANANDA INSTITUTE OF PROFESSIONAL STUDIES TECHNICAL CAMPUS.

Keywords: Aadhaar, Privacy, Surveillance, Data Protection, Digital Identity.

INTRODUCTION

Digital identity regimes have emerged as a defining characteristic of twenty-first-century governance.¹ These large-scale regimes, based on extensive biometric and demographic data, are promoted as mechanisms to improve welfare delivery, prevent financial crime, and increase administrative efficiency across multiple domains.² The Aadhaar programme, India's digital ID scheme, captures both the opportunities and challenges in such systems. However, these promises are consistently accompanied by persistent questions of privacy and the basic protection of fundamental civil rights, particularly the absence of strong legal safeguards.

The constitutional establishment of the inherent right to privacy in *K.S. Puttaswamy v. Union of India* (2017) constituted an irrefutable turning point in the panorama of Indian jurisprudence.³ The Supreme Court, by its unanimous judgment, strongly emphasised that every measure of the State, including those entailing widespread monitoring and sophisticated identification systems, shall rigorously undergo the test of proportionality to remain constitutionally sound and legitimate. But the subsequent confirmation of Aadhaar's constitutionality in *Puttaswamy* (2018), while accompanied by significant limitations and safeguards, enunciates emphatically the uneasy and oftentimes precarious balance between the state's pressing interests in efficiency and effective governance, and individuals' equally pressing interests in privacy and autonomy.⁴

Across the world, leading systems such as the General Data Protection Regulation (GDPR) of the European Union and the Council of Europe's Convention 108+ are collaborative efforts to regulate the acceleration of technological progress with stern data protection standards.⁵ India, on the other hand, has recently passed the Digital Personal Data Protection Act, 2023.⁶ This

¹ ID2020 Alliance, *Alliance Manifesto* (2018) <https://www.id2020.org/assets/pdf/ID2020-Alliance-Manifesto.pdf> accessed 14 September 2025

² World Economic Forum, *Insight Report: Identity in a Digital World – A New Chapter in the Social Contract* (2018) 5 https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf accessed 14 September 2025.

³ *K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

⁴ *K S Puttaswamy v Union of India* (2019) 1 SCC 1

⁵ European Union, Regulation (EU) 2016/679, *General Data Protection Regulation* [2016] OJ L 119/1; Council of Europe, 'Convention 108+: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (2018) <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> accessed 14 September 2025.

⁶ Digital Personal Data Protection Act 2023, No 22, Acts of Parliament, 2023

asymmetrical and ongoing making of regulation, therefore, poses pressing and profound questions about whether India's expanding digital ID architecture adequately safeguards constitutional rights or, worse, arguably comes to insidiously institutionalise a pervasive mode of surveillance governance within its democratic order.⁷

This essay analyses the complex constitutional and governance aspects of Indian digital ID regimes, situating Aadhaar and its related initiatives within the broader and critical privacy discourse. By focusing keenly on the inherent tensions between administrative efficiency, social integration, and the overriding need to protect individual rights, the analysis addresses the central research question: how can India design and regulate its expanding digital identity infrastructure to uphold civil liberties and individual autonomy while achieving legitimate and requisite state objectives?

CONSTITUTIONAL FRAMEWORK AND PRIVACY JURISPRUDENCE IN INDIA

The recognition of privacy as a constitutional right in Justice K.S. Puttaswamy (Retd.) v Union of India was a constitutional benchmark within the Indian legal fraternity. The nine-judge bench, by consensus, reaffirmed that privacy is a part of liberties and dignity under Article 21 of the Constitution and pervades other constitutional rights such as equality and freedom of speech.⁸ This jurisprudence supplied the normative basis to challenge state-led digital identity regimes like Aadhaar and new health and welfare-linked IDs.

The major decision in Puttaswamy was to take on board the proportionality test. Government intrusions into privacy are required to (i) have a legitimate goal, (ii) be reasonably connected to that goal, (iii) be the least restrictive option, and (iv) have proportionality between the goal sought and the rights restricted.⁹ But successive state surveillance and identification policies have usually failed to meet these standards. For instance, Central Monitoring System (CMS) and Aadhaar-based authentication systems operate without a strong judicial or parliamentary accountability structure, hence creating issues about constitutionality.¹⁰

⁷ MediaNama, 'A Complete Guide to India's Digital Personal Data Protection Bill, 2023' (18 August 2023) <https://www.medianama.com/2023/08/223-complete-guide-indias-digital-personal-data-protection-bill-2023/> accessed 14 September 2025.

⁸ *K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

⁹ *Ibid.*

¹⁰ Usha Ramanathan, 'Biometrics Use for Social Protection Programmes in India Risk Violating Human Rights of the Poor' (Social Protection and Human Rights, 2014) <https://socialprotection-humanrights.org/expertcom/biometrics-use-for-social-protection-programmes-in-india-risk-violating-human-rights-of-the-poor/> accessed 14 September 2025.

Further, while the Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first comprehensive data protection statute, it has been condemned for its pervasive exemptions in the state's favour.¹¹ The Central Government, under Section 17 of the Act, can exempt any of its instrumentalities from operation where it is required in the interests of sovereignty, integrity, or security of the state.¹² The sweeping carve-outs thus defeat the constitutional requirement of necessity and proportionality set out in *Puttaswamy*, and have the potential to create a judicial landscape where surveillance becomes the new normal.

Similarly important is the lack of an independent data protection agency with strong enforcement powers. The DPDP Act makes provision for the establishment of the Data Protection Board of India, but its appointment and removal are in the hands of the executive.¹³ This design may weaken its independence, rendering it less effective at protecting privacy when faced with far-reaching state-backed digital ID systems.

GOVERNANCE AND SECURITY-BASED MONITORING THROUGH DIGITAL ID SYSTEMS

Indian digital identification systems, particularly Aadhaar, are one of the pillars of governance and people's welfare. Aadhaar is connected with schemes as diverse as food provision, banking and telecommunication, building a huge centralised store of biometric and demographic information.¹⁴ Although the declared aim is to deliver services efficiently, connecting Aadhaar with various state activities opens up major privacy issues, particularly against the backdrop of the Supreme Court's affirmation of privacy as a basic right in *K.S. Puttaswamy v. Union of India* (2017).¹⁵

The ambit of digital ID monitoring goes beyond welfare administration. Security and law enforcement programs like the Central Monitoring System (CMS), National Intelligence Grid (NATGRID), and the Automated Facial Recognition System (AFRS) are increasingly based

¹¹ Internet Freedom Foundation, *Monsoon 2023 Legislative Brief* (August 2023) https://content.internetfreedom.in/api/files/divco3ywedt9rpe/c8qqmb656hhybnk/monsoon_2023_legislative_brief_z54yMuKQXW.pdf accessed 14 September 2025.

¹² Digital Personal Data Protection Act 2023, s 17.

¹³ MediaNama, 'Scope of Data Protection Board under India's Digital Personal Data Protection Bill' (3 August 2023) <https://www.medianama.com/2023/08/223-india-data-protection-board-personal-data-bill/> accessed 14 September 2025.

¹⁴ Centre for Internet and Society, 'FAQ on the Aadhaar Project and the Bill' (2016) <https://cis-india.org/internet-governance/blog/aadhaar-project-and-bill-faq> accessed 14 September 2025.

¹⁵ *K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

on Aadhaar-linked data to enable tracking and profiling.¹⁶ The 2023 deployment of facial recognition systems by law enforcement agencies like the Delhi Police demonstrates the growing use of biometric surveillance technology in administration and has sparked worries about bulk collection of data and the absence of statutory protections.¹⁷ Civil liberties groups contend that India's growing surveillance apparatus, such as database interlinkages and digital ID schemes, violates the constitutional test of proportionality because it lacks adequate judicial supervision and statutory protection.¹⁸

Governance-based IDs are also spreading into new areas. The Ayushman Bharat Digital Mission recommends a National Digital Health ID, and the government has already signalled a National Social Registry, which would integrate data between ministries.¹⁹ The Digital Personal Data Protection Act, 2023, is not quite enough to safeguard citizens against misuse of surveillance since it exempts the state from adhering to it in the name of "sovereignty and integrity of India" or "public order."²⁰ This broad carve-out, combined with the lack of meaningful redressal mechanisms, allows the state to expand ID-based governance into fields that have a direct bearing on fundamental rights.

The supporters of Aadhaar and other digital IDs say that they enhance efficiency and reduce fraud. Yet, the substantive risks of such as profiling, denial of welfare for failing to authenticate, stifling of dissent, and the possible reorientation towards surveillance tools should not be set aside.²¹ The absence of a robust statutory basis, akin to the GDPR of the European Union, means Indian citizens have few safeguards against the abuse of their digital identity information.²²

¹⁶ Pranesh Prakash, 'Surveillance in India: Policy and Practice' (Centre for Internet and Society, 2014) <https://cis-india.org/internet-governance/news/surveillance-in-india-policy-and-practice> accessed 14 September 2025.

¹⁷ Internet Freedom Foundation, *Monsoon 2023 Legislative Brief* (August 2023).

¹⁸ *Ibid.*

¹⁹ Ministry of Health and Family Welfare, 'Ayushman Bharat Digital Mission' (Government of India, 2021); Vikaspedia, 'Ayushman Bharat Digital Mission Overview' (2021) <https://en.vikaspedia.in/viewcontent/health/health-care-innovations/ayushman-bharat-digital-mission-health-care-innovations-1/ayushman-bharat-digital-mission> accessed 14 September 2025.

²⁰ Digital Personal Data Protection Act 2023, s 17.

²¹ Usha Ramanathan, 'Biometrics Use for Social Protection Programmes in India Risk Violating Human Rights of the Poor' (Social Protection and Human Rights, 2014).

²² European Union, Regulation (EU) 2016/679, (General Data Protection Regulation), arts 12–22.

INTERNATIONAL AND COMPARATIVE ANALYSIS OF DIGITAL ID AND PRIVACY

Digital ID schemes are not unique to India, and are also being launched across the globe with the same challenges between efficiency and civil liberties. Under the European Union setup, standards safeguarding data are established within the General Data Protection Regulation (GDPR), which comprehensively governs collecting, processing, and transferring personal data.²³ The rights-based approach in GDPR makes sure that the individuals themselves are in control of their information, such as the right to information, right to erasure and ban on automated profiling.²⁴ The Aadhaar regime in India does not have such protections, especially in terms of state surveillance and exceptions under the Digital Personal Data Protection Act, 2023.²⁵

The Council of Europe Convention 108+ also advances worldwide privacy principles, imposing binding obligations on signatory countries to protect citizens from misuse of automated personal data processing.²⁶ India is not a signatory, yet the convention calls attention to the increasing understanding that privacy needs to stay at the heart, even in digital government. It has been argued that Convention 108+ should be expanded into a worldwide treaty, but as yet, only Europeans and a few non-members have joined.²⁷

In parallel, the OECD Declaration on Government Access to Data (2022) has tried to standardise transparency and protections when states request access to personal data for national security or law enforcement.²⁸ The agreement is directly applicable to India's Digital ID governance: it illustrates how democratic systems can recognise state security requirements without giving the state blanket exemptions. India's existing method, on the other hand, provides the state absolute freedom to circumvent safeguards, diluting accountability and public trust.²⁹

²³ Ibid.

²⁴ European Data Protection Supervisor, 'Rights of the Individual' https://www.edps.europa.eu/data-protection/our-work/subjects/rights-individual_en accessed 14 September 2025.

²⁵ Digital Personal Data Protection Act 2023, s 17.

²⁶ Council of Europe, 'Convention 108+: Convention for the protection of individuals with regard to the processing of personal data' (2018).

²⁷ Graham Greenleaf, 'Modernised Data Protection Convention 108 and the GDPR' (UNSW Law Research Series, 2019) <https://classic.austlii.edu.au/au/journals/UNSWLRS/2019/3.pdf> accessed 14 September 2025.

²⁸ OECD, 'Declaration on Government Access to Personal Data Held by Private Sector Entities' (14 December 2022) https://www.ppc.go.jp/files/pdf/government_access_en.pdf accessed 14 September 2025.

²⁹ Internet Freedom Foundation, *Monsoon 2023 Legislative Brief* (August 2023).

The comparative framework indicates that India's regime is that of an outlier. While Europe and OECD nations are gravitating toward greater accountability and people-centric protections, India's application of broad state exemptions assumes a model of state effectiveness and power over citizen rights. The companion precedent is GDPR Article 23, which sets out specific and narrow circumstances in which individual rights can be limited. These restrictions include matters of national security or public interest objectives, but must be necessary, proportionate, and subject to adequate safeguards. India's Digital Personal Data Protection Act, on the other hand, allows broader exemptions without such tight restrictions. For example, whereas GDPR is specific regarding strict protocols, India leaves broader latitude to the state, yet again accentuating the divergence. This progress highlights India's embracing of international best practices wherein digital IDs engage citizens, yet don't expose them to unregulated spying.

BALANCING NATIONAL SECURITY AND CIVIL LIBERTIES

The utilisation of Digital ID systems, set up in nations such as Aadhaar in India, is generally authorised by the government pursuant to standards of good governance and increased national security. Governments argue that with accurate identification established, these systems assist in reducing welfare fraud, counter money laundering, and assist in counter-terrorism initiatives.³⁰

But the same infrastructure used to support the government can weaken civil liberties as well. In affirming the constitutionality of Aadhaar in *K.S. Puttaswamy v Union of India (Aadhaar)*, the Indian Supreme Court recognised that allowing databases to be connected might raise surveillance issues if sufficient protection is not instituted.³¹ That recognition is of a continued constitutional tension between the protection of privacy under Article 21 and the state's search for security and welfare goals.³²

Internationally, the United Nations Human Rights Council has warned that surveillance policies, though within the bounds of security, need to adhere to principles of necessity, proportionality, and legality.³³ Abuses of Digital IDs in monitoring political opinions or stifling

³⁰ Centre for Internet and Society, 'FAQ on the Aadhaar Project and the Bill' (2016) <https://cis-india.org/internet-governance/blog/aadhaar-project-and-bill-faq> accessed 14 September 2025.

³¹ *K S Puttaswamy v Union of India* (2018) 1 SCC 809

³² Constitution of India, art 21.

³³ United Nations Human Rights Council, *The Right to Privacy in the Digital Age*, A/HRC/RES/42/15 (2019).

dissent, as identified in human rights research, are a danger of democratic regression where security needs override basic freedoms.³⁴

Achieving balance, therefore, involves a recognition that the problem is not necessarily a "trade-off" between security and privacy, but a reconceptualisation of constitutional principles in the information age. As scholars noted, unregulated data concentration in state systems generates a "function creep," where identification technologies spread into new realms beyond their initial purpose, compromising individual autonomy.³⁵ At the same time, security issues cannot be dismissed; states remain obligated to make virtual economies secure, avoid fraud, and promote safety in a world full of interdependence.

The legal problem at the core is how to create protections that avoid arbitrary surveillance while recognising legitimate governance goals fulfilled by Digital ID systems. Lacking protections, the very mechanisms that have been created to provide greater security threaten to destroy the constitutional order that they are designed to serve.

RECOMMENDATIONS

A balanced regulatory framework for Digital ID systems must preserve privacy without overly stifling the genuine goals of governance and security. Several measures, prioritised by impact and feasibility, are required:

Enforcing rigorous data protection policies: While the Digital Personal Data Protection Act, 2023, provides a starting point, it lacks an independent regulator.³⁶ There is a need for a truly independent Data Protection Authority with enforcement powers. The EU General Data Protection Regulation (GDPR) is a comparative model highlighting how independent regulation can foster accountability.³⁷

Enhancing parliamentary and judicial oversight: Surveillance authorities linked to Digital IDs need to be under the scrutiny of independent judicial review according to the

³⁴ Council of Europe, 'Convention 108+: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018).

³⁵ OHCHR, 'Spyware and Surveillance: Threats to Privacy and Human Rights Growing – UN Report' (16 September 2022)

<https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report> accessed 14 September 2025.

³⁶ Internet Freedom Foundation, *Monsoon 2023 Legislative Brief* (August 2023).

³⁷ European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), arts 12–22.

proportionality principle articulated in *Puttaswamy* (2017).³⁸ Parliamentary committees should also oversee implementation to prevent executive overreach.³⁹

Integrating privacy-by-design into Digital ID infrastructures: Technical solutions like decentralised storage, purpose limitation and anonymisation must be built into Aadhaar and other Digital ID designs.⁴⁰ This is best practice in global affairs, as noted by the UN Special Rapporteur on Privacy.⁴¹

Strengthening people's remedies: Citizens must be informed whenever their data is accessed, and there should be a right to complain about unauthorised surveillance or omission. Inadequate redressal facilities under Aadhaar and the Data Protection Act leave people vulnerable to abuse of the system.⁴²

Avoiding function creep: The expansion of Aadhaar to policing, telecom, and banking for welfare must be closely limited by legal protections.⁴³ The Council of Europe has noted that mass data linking facilitates aggressive profiling and encroaches on privacy norms.⁴⁴

Bringing it in line with international standards: India will have to come at the evolving global frameworks, such as Convention 108+ and the OECD agreements relating to the protection of privacy in law enforcement, to align domestic policy with the international standard.⁴⁵

Collectively, these reforms can mitigate the risk of a surveillance-oriented democracy and ensure that Digital ID systems achieve governance objectives without compromising constitutional rights.

³⁸ *K S Puttaswamy v Union of India* (2017) 10 SCC 1.

³⁹ Centre for Internet and Society, 'FAQ on the Aadhaar Project and the Bill' (2016).

⁴⁰ OHCHR, 'Spyware and Surveillance: Threats to Privacy and Human Rights Growing – UN Report' (16 September 2022).

⁴¹ UN Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, A/HRC/46/37 (2021).

⁴² Internet Freedom Foundation, *Monsoon 2023 Legislative Brief* (August 2023).

⁴³ *K S Puttaswamy v Union of India* (2018) 1 SCC 809

⁴⁴ Council of Europe, 'Convention 108+ : The Modernised Version of a Landmark Instrument' (2018) <https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108> accessed 14 September 2025.

⁴⁵ OECD, 'Declaration on Government Access to Personal Data Held by Private Sector Entities' (14 December 2022); Council of Europe, 'Convention 108+: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018).

CONCLUSION

The path of Digital ID systems in India shows both the potential and danger of technology-led governance. Aadhaar and associated programs have undoubtedly increased welfare delivery, financial inclusion, and bureaucratic efficiency.⁴⁶ But their spread from primary welfare use to law enforcement, banking, and private sector applications presents constitutional issues.⁴⁷ The Puttaswamy jurisprudence establishes privacy as a fundamental right, but the governance-based surveillance reality indicates a persistent tension between rights and state needs.⁴⁸

The lack of adequate institutional protection heightens this tension. The Digital Personal Data Protection Act, 2023, is a step in the right direction, but it falls short of providing the autonomy required to prevent executive abuse.⁴⁹ In the absence of explicit boundaries on function creep, the threat of "surveillance democracy" becomes tangible, where efficiency is used as a cover for eroding civil liberties.⁵⁰ Comparative cross-border systems, such as the GDPR and Convention 108+, prove it is achievable to harmonise governance and innovation with robust rights protection.⁵¹ India's hesitation to extend similar protections puts its people at a structural disadvantage globally.⁵²

Ultimately, welfare, privacy, and security should not be viewed as mutually exclusive objectives. Incorporating privacy-by-design, instituting effective oversight, and aligning with international best practices can enable India to realise the benefits of Digital IDs without undermining its constitutional commitment to freedom.⁵³ The debate surrounding Digital ID thus centres on the fundamental character of India's democracy rather than on technological advancement alone.

⁴⁶ Centre for Internet and Society, 'FAQ on the Aadhaar Project and the Bill' (2016).

⁴⁷ *K S Puttaswamy v Union of India* (2018) 1 SCC 809.

⁴⁸ *K S Puttaswamy v Union of India* (2017) 10 SCC 1.

⁴⁹ Internet Freedom Foundation, *Monsoon 2023 Legislative Brief* (August 2023).

⁵⁰ OHCHR, 'Spyware and Surveillance: Threats to Privacy and Human Rights Growing – UN Report' (16 September 2022).

⁵¹ Council of Europe, 'Convention 108+: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018).

⁵² OECD, 'Declaration on Government Access to Personal Data Held by Private Sector Entities' (14 December 2022).

⁵³ United Nations Human Rights Council, Report of the Special Rapporteur on the Right to Privacy A/HRC/46/37 (2021).