



LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.334>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

CENTRALISATION OF BIRTH AND DEATH RECORDS: DIGITAL STATE CAPACITY, PRIVACY AND COMPARATIVE DATA GOVERNANCE MODELS

Phalak Lamba¹

I. ABSTRACT

Civil registration of births and deaths is a foundational State function, but its increasing digitisation and centralisation raise a distinct constitutional question: how far may the State aggregate, link, share and reuse population-scale civil-registration data beyond the immediate purposes for which it is collected? Birth and death records support legal identity, public administration, demographic planning and the delivery of public services, yet their integration across government databases can also intensify risks to informational privacy, purpose limitation and institutional accountability. This paper examines these concerns through doctrinal, analytical and comparative legal research. It analyses the Registration of Births and Deaths Act, 1969, as amended in 2023, the constitutional right to privacy recognised in Justice K.S. Puttaswamy (Retd.) v. Union of India and developed in the Aadhaar litigation, and the Digital Personal Data Protection Act, 2023 together with the Digital Personal Data Protection Rules, 2025 and their phased implementation. The paper focuses not on the legitimacy of statutory civil registration itself, but on the downstream storage, aggregation, interoperability, sharing and secondary use of the resulting data. It finds that administrative necessity at the point of registration does not, by itself, justify unrestricted subsequent dissemination or reuse. Comparative analysis of Estonia, the European Union and the United Kingdom further demonstrates that effective digital government need not depend upon indiscriminate data concentration. The paper therefore proposes a model of accountable interoperability in which data exchange is governed by clearly defined statutory purposes, data minimisation, role-based access, auditable transaction logs, retention discipline, correction mechanisms, layered security and independent oversight. Such an architecture can

¹ LL.M. (Business Law) Student at Lovely Professional University, Punjab (India). Email: phalaklamba@gmail.com

strengthen Digital State Capacity while preserving constitutional limits on governmental informational power.

II. KEYWORDS

Civil Registration; Informational Privacy; Digital State Capacity; Function Creep; Accountable Interoperability.

III. INTRODUCTION

The registration of births and deaths may seem on the surface a trivial administrative task. However, on a legal and institutional scale, it plays a groundbreaking function. A birth record is used to confirm facts about a person's date and place of birth and other legally relevant details; a death record is used to record the end of a person's legal personality and to enable estate administration, succession, insurance and demographic statistics. The population level, Civil registration is used to make the State aware of demographic change and to provide data to support planning, public administration and official statistics. The constitutional role of civil registration is therefore unique: it deals with very private events but its systematic management is a legitimate and, and sometimes required, public role.

The actual and thus constitutional relevance of this activity is altered by digitization. The local paper-based register is difficult to combine, search or aggregate with other databases, and the "friction of physical distance" and the time it takes to physically retrieve the register have been an informal safeguard. Whereas the digital record is capable of being queried, copied, exchanges and even at high scale be linked simultaneously across different across institutional boundaries. There may therefore be real administrative benefits as a result of centralization, for example, the elimination of duplication, the updating of records, the better co-ordination of public bodies and the timelier and more accurate production of statistics.

It is very pertinent to understand that the aggregation changes the very nature of the government knowledge. The data which is harmless on its own can be much more

revealing when it is aggregated across different institutions and tied to welfare, identity, education, tax or other administrative systems. The legal issue, however, is not just whether birth and death records can be taken but the status of registration itself is based on longstanding statutory requirements. The question of the hour is what will happen to the information once it is collected and what type of legal architectural framework will regulate it?

The legal framework of the Registration of Births and Deaths Act, 1969 formulates a basic structure for the registration of births and deaths all across India, covering all the areas from registrar general of India to chief registrar's state wise and local registrars². The amendment act, 2023 is very salient as it provides the need for the national database for the registration of birth and death to be maintained in India maintained by the registrar general of India and at state level the obligation is upon chief registrar and further to share information about registration data with the database.³

The Registration of Births and Deaths (Amendment) Bill, 2023 was introduced in the Lok Sabha on 26 July 2023, passed by the Lok Sabha on 1 August 2023 and by the Rajya Sabha on 7 August 2023. It received the assent of the President on 11 August 2023 and came into force on 1 October 2023.⁴ This amendment should be read carefully, however. The creation of the national database is not an answer to all questions relating to access, secondary use, retention and interoperability; when analyzing the constitution, one must distinguish between what Parliament has expressly authorized and what may become technically possible, with the database being rolled out.

² The Registration of Births and Deaths Act, 1969 (Act No. 18 of 1969) §§ 3-4, India Code, <https://www.indiacode.nic.in> (last visited Sept. 13, 2026).

³ The Registration of Births and Deaths (Amendment) Act, 2023 (Act No. 20 of 2023), amending § 3A of the principal Act; PRS Legislative Research, *The Registration of Births and Deaths (Amendment) Bill, 2023*, <https://prsindia.org/billtrack/the-registration-of-births-and-deaths-amendment-bill-2023> (last visited Sept. 13, 2026).

⁴ Registration of Births and Deaths (Amendment) Act, 2023, No. 20 of 2023 (India); Registration of Births and Deaths (Amendment) Bill, 2023, Bill No. 93 of 2023 (introduced in Lok Sabha July 26, 2023); PRS Legislative Research, *The Registration of Births and Deaths (Amendment) Bill, 2023*; Office of the Registrar General, India, Ministry of Home Affairs, S.O. 4058(E), *Gazette of India, Extraordinary* (Sept. 13, 2023) (India).

This distinction took on greater significance after recognizing privacy as a fundamental right. The nine-judge Bench of Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India⁵ unanimously declared that privacy is a right guaranteed by Part III of the Constitution and the right to informational privacy is an important aspect of individual liberty and dignity. The judgment⁶ that followed on Aadhaar provided a glimpse of the State's legitimate interest in technological systems on a scale of the population and the constitutional significance of statutory purpose, proportionality and ensuring the process was protected. The principles are not an attack on the unconstitutionality of government databases; they are an attack on the design and operation of government databases that is never out of bounds.

For this reason, this paper makes a limited but important proposition that Digital State Capacity is a legitimate and valuable governmental goal, but that more technical capacity does not mean more legal bounds of governmental data power. The entirety of the data life cycle – not just the moment of registration – is the unit of analysis that is relevant to the Constitution. It is very much possibility that system can work perfectly legal when it collected the data but there is no doubt that there could be time when it could raise significant constitutional issues at the time of the subsequent application and aggregation. The problem that Indian law faces is that it needs to ensure that there is a purpose limitation, accountability and institutional restraint architecture that accompanies administrative modernization of civil registration.

A. Statement of the Problem

The shift towards civil registration in India takes place between the capacity of the administration and limitation of information. While centralized databases can enhance coordination and public administration, they can also produce a long-term (durable) searchable database of population-level information about some of the most fundamental events in an individual's life. This paper explores the question of whether the statutory

⁵ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

⁶ K.S. Puttaswamy v. Union of India (Aadhaar-5J.), (2019) 1 SCC 1 (India).

and institutional structure that provides regulation for this concentration of information has adequate boundaries for collection, access, sharing, retention and secondary use. A solution to this problem would not be possible if we treated privacy and efficiency as value-antagonistic. A constitutionally sound data-governance mechanism needs to ask the question of when efficiency is a proper aim, whether it really needs to be centralized to that extent to attain that efficiency, whether there are less intrusive structures that can produce that efficiency, and what institutional protections are needed to guard against function creep and unchecked informational power.

B. Research Questions and Objectives

1. Research Questions

This paper addresses the following research questions:

- How does Digital State Capacity in India benefit from the centralisation and digitisation of birth and death records?
- What is the existing legal and institutional framework governing civil registration in India, and how has the Registration of Births and Deaths (Amendment) Act, 2023 altered that framework?
- How do the constitutional principles of privacy articulated in *Justice K.S. Puttaswamy (Retd.) v. Union of India* and the Aadhaar litigation apply to the centralisation and use of civil-registration information?
- What legal and governance risks arise from data aggregation, interoperability, function creep, security failures and inaccurate civil-registration records?
- To what extent does the Digital Personal Data Protection Act, 2023, read with the Digital Personal Data Protection Rules, 2025, govern the State's processing of civil-registration data, including the applicable statutory grounds, exemptions and phased commencement of the framework?

- What lessons can India draw from the data-governance models of Estonia, the European Union and the United Kingdom?
- How can informational autonomy and administrative capacity be balanced in the design and governance of a national civil-registration database?

2. Research Objectives

The objectives of this paper are to examine the Indian statutory and institutional framework governing birth and death registration; to analyse the transition from local registration to digitised and increasingly integrated data infrastructure; to assess State databases from the perspective of Digital State Capacity; to examine the constitutional implications of the aggregation and centralisation of personal information; to evaluate the relevance of the DPDP framework to public-sector processing of civil-registration data; to compare selected models of data governance and identify transferable institutional lessons; and to propose legally feasible safeguards for an accountable civil-registration system.

C. Research Methodology, Scope and Limitations

1. Methodology

This paper has been written in a doctrinal, analytical and comparative method of legal research. It is based largely on the work of the available primary resources like books and official publications and does not involve field surveys or interviews ie the empirical survey has not been done, because the subject matter involves interpreting the text of the constitution, statutes, subordinate legislation and judicial precedent.

The doctrinal component of the research focuses on the different provisions of the Constitution of India and then the primary central laws such as the Registration of Births and Deaths Act, 1969 and the Registration of Births and Deaths (Amendment) Act, 2023, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the Information Technology Act, 2000, and then interpretation of the leading Supreme Court decisions.

The analytical aspect of the paper examines if the legal architecture of centralization is in consonance with the constitutional principles of legality, legitimate purpose, necessity, proportionality and procedural safeguards laid out in Puttaswamy. The comparative element looks at Estonia, the European Union and the United Kingdom, as they each address a specific question: how are interoperable digital infrastructures established, how is a vocabulary of data-protection principles developed, and how is data governance established for civil-registration data.

2. Scope

The principal jurisdiction analysed in this paper is India. The paper concentrates in particular on birth and death records and not on the broader scope of civil-status records such as marriage or adoption records, although if relevant to the statutory scheme, these are mentioned. It does not seek to make a technical audit of the Civil Registration System or an empirical assessment of cybersecurity vulnerabilities, for such an audit would involve access to non-public technical information that is beyond the scope of doctrinal legal research.

The comparative study is functional and not comprehensive; it introduces concepts and models of law and institutions that are relevant to the Indian problem without suggesting that foreign institutions can be imported without awareness of India's unique constitutional framework, federal system and administrative environment.

3. Limitations

The research is drawn from publicly available laws, official documents, government reports and reported judicial documents as of September 2026. It is not based on interviews, surveys or fieldwork. The practices involved in technical implementation may change more quickly than laws, and State-level rules and administrative circulars may vary by jurisdiction or may not be captured here. The paper thus differentiates, where appropriate, between settled conclusions of law and policy recommendations for the future, and between an ability to act legally and a legal power.

IV. CONCEPTUAL FRAMEWORK

1. Civil Registration

Civil registration can be seen as the ongoing, permanent, compulsory and universal filing of vital events in line with legal mandates⁷. It is important because of the twofold nature of the records it generates. They facilitate the registration of civil acts (identity, relationship, age, succession) and they also produce information related to civil administration and official statistics. Both civil registration as a whole and civil registration of the individual is legitimate object of State organization. The public nature of the system does not, however, negate the personal nature of the information in it.

2. Centralization, Digitization and Interoperability

Centralization does not necessarily equal digitization. Centralization relates to the institutional and technical place of control, storage or access, while digitization is the process of putting records in electronic format. A digitized system can be part of a system with files held in different institutions, and federated can allow files to be shared without having a single file in one location that contains all copies of all files. Interoperability, on the other hand, should not be confused with free sharing. Instead, it could be created by deliberate interfaces, access controls, transaction logging and targeted requests. This separation is important to the current analysis, since technological architecture could inhibit or expand the governmental informational power, whether or not it is prescribed by law.

3. Digital State Capacity

For the purpose of this paper, Digital State Capacity is defined as the capacity of public institutions with the capability of using Digital infrastructure, information and organizational systems to effectively undertake their legally mandated functions. It encompasses trustworthy documentations, coordination among institutions, technical

⁷ Cf. United Nations, Principles and Recommendations for a Vital Statistics System, Statistical Papers Series M No. 19/Rev.3, U.N. Doc. ST/ESA/STAT/SER.M/19/Rev.3 (2014).

facilities, data quality, responsiveness, and provision of services efficiently. The idea should not be limited to the amount of information the State has. A competent digital state must also have reliable and up-to-date records, legal procedures, institutional capacity and ways to fix mistakes. Capacity can be created but without accountability, it can create power and not legitimate governance.

4. Informational Privacy and Informational Autonomy

Informational privacy involves the individual's interest in who has access to his or her personal information, or who does not have access to it, and/or what is done with it. The concern doesn't only apply to a governmental setting: The information may have been lawfully released by one authority for one purpose and then be used in a constitutionally problematic way when added together and/or repurposed for another purpose. Informational autonomy thus focuses on context, purpose and control, rather than disclosure alone. The Supreme Court has recognised that information which may appear inconsequential when held in separate silos can, when aggregated, reveal a detailed picture of an individual's personality and behaviour, thereby intensifying concerns relating to informational privacy.⁸

5. Function Creep

Creep means a progressive growth of a database or technology system beyond its original legal scope of authority. It is especially applicable in situations where a basic database is made attractive for other purposes than those foreseen at its inception, such as verifying identities, assessing eligibility, checking for fraud, or other non-obvious administrative purposes. Not all use extensions are illegitimate; many are quite legal and useful. The constitutional issue is raised when the use is new and the legal basis is not sufficiently clear or no new necessity and proportionality analysis, or insufficient safeguards. Therefore, no longer to be seen as a given fruit of digitization, function creep is rather

⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶¶ 170, 175 (*Chandrachud, J.*) (India).

best viewed as a governance risk, stemming from the confluence of retained data and growing institutional demands.

V. THE INDIAN LEGAL AND INSTITUTIONAL FRAMEWORK

A. The Registration of Births and Deaths Act 1969

The Registration of Births and Deaths Act 1969⁹ is the main legislation of registration in India. Registration of births and deaths is under Entry 30 of the Concurrent List of Seventh Schedule of the Constitution, which empowers Parliament and State Legislatures to enact laws on the subject, but the 1969 Act continues to be the central legislation, with State rules applying it¹⁰.

The structure of the Act sets up a hierarchy of registrations with the Registrar General of India, Chief Registrars appointed by States and local Registrars; and the procedure for registration, keeping of records and compilation of vital statistics. The statutory structure highlights that, throughout history, civil registration has been a matter of both local administration and national coordination; in today's context, the question is to what extent does digital technology influence the actual and constitutional implications of this coordination.

The Act imposes legal obligations on certain persons and institutions with regard to registering, lays down the requirement of registering births and deaths within 21 days of their occurrence and gives the certificate of registration¹¹.

It should not be over-emphasized that the Act is not a general data-sharing charter, but rather a civil-registration act. Hence, any possibility that arises as to the access to the resulting database should be based on the wording of the Act and/or subordinate rules

⁹ The Registration of Births and Deaths Act, 1969 (Act No. 18 of 1969), India Code.

¹⁰ India Const. sch. VII, list III, entry 30; PRS Legislative Research, The Registration of Births and Deaths (Amendment) Bill, 2023, <https://prsindia.org/billtrack/the-registration-of-births-and-deaths-amendment-bill-2023> (last visited Sept. 13, 2026).

¹¹ Registration of Births and Deaths Act, 1969, §§ 8-13.

or on other valid legal basis and not only on the fact of the existence of the digital database.

B. The Registration of Births and Deaths (Amendment) Act, 2023

The amendment in 2023 is a significant change to the statutory framework of civil registration. The amendments in the act brought for the establishments of the national register of births and deaths by the Register general of India compulsorily and further the 2023 act and mandated that all the chief registrars also need to provide the data on birth and deaths to the database while requiring the Chief Registrars to maintain corresponding databases at the State level, and the Amendment Act came into force on 1 October 2023.¹²

Most important, sub-section (5) of the amended section 3A says that the national database shall be shared with authorities for the preparation or maintenance of any other of the specified databases or any other database notified by the Central Government upon request and prior approval of the Central Government¹³. At the state level, there may be databases that are shared with State-approved authorities. This is the only aspect in the 2023 amendment that is constitutionally relevant, as it establishes an explicit statutory linkage (although one that is centrally controlled) between the civil-registration database and some of India's other large administrative and identity databases.

The amendment also enhances the evidence value of the birth certificate by making it the sole principal document to establish the date and place of birth of a person born after the Act came into force, for specific purposes such as school enrollment, driving licence,

¹² Office of the Registrar General, India, Ministry of Home Affairs, S.O. 4058(E), Gazette of India, Extraordinary (Sept. 13, 2023) (India).

¹³ The Registration of Births and Deaths (Amendment) Act, 2023 § 4 (inserted § 3A(5)); PRS Legislative Research, *supra* note 8; IMPRI Impact and Policy Research Institute, Registration of Births and Deaths (Amendment) Act, 2023, <https://www.impriindia.com/insights/birth-death-act/> (last visited Sept. 13, 2026).

electoral roll preparation, marriage registration, appointment to a government office and passport issuance¹⁴.

The amendment has at least two distinct constitutional significance. First, it shifts the institutional level used to collect and hold civil-registration data from the small-scale and fragmentary storage of data in State and local offices to the creation of a truly national database. Secondly, it explicitly enables linking of that data with other large-scale national registers such as the population register, electoral roll and Aadhaar ecosystem, which is a very real prospect and not just a figment of the imagination.

However, a comprehensive analysis should be done without committing to a common mistake, as the registration data is not necessarily automatically available in the same way to all government databases. The analysis of the legal basis must focus on the specific gateway in section 3A (5) that is relied upon for each individual sharing, because the mere fact of a national database does not automatically give legal authority to all sharing, but depends on the specific sharing envisaged.

The introduction of the 2023 amendment states that the goal is to establish national and State-level databases that could be used to update other databases and make public services and the delivery of social-welfare more efficient, accurate and transparent, and to limit duplication and errors in Indian's multiple databases¹⁵.

These are legitimate and important objectives. They do not, however, rule out the need for purpose limitation. The structure of administration of information is subject to constitutional review, but a statute can properly prescribe a specified administrative task and leave the techniques for aggregation and then use of information to the constitutional review.

¹⁴ The Registration of Births and Deaths (Amendment) Act, 2023 § 3; see also Rau's IAS, The Registration of Births and Deaths (Amendment) Act, 2023, <https://compass.rauias.com/current-affairs/registration-births-deaths-amendment-act-2023/> (last visited Sept. 13, 2026).

¹⁵ Statement of Objects and Reasons, The Registration of Births and Deaths (Amendment) Bill, 2023, Bill No. 93 of 2023; Rau's IAS, *supra* note 15.

C. The Civil Registration System

The Civil Registration System is a framework for statutory registration, which is implemented in India through a combination of national coordination and State/local implementation: the amendment of 2023 also mandates the States to register on the Civil Registration System portal of the Centre and also to provide data to the Registrar General of India¹⁶.

The multi-level design has direct implications for the debate on centralization: it shows that administrative functions can be decentralized even if there are national standards and a national information system. The normative issue is, then, not just whether a system is 'centralized' or 'decentralized' broadly, but what decisions are made, and what particular operations on the data, at each institutional level, and subject to what controls.

D. Digital Personal Data Protection Framework

The Digital Personal Data Protection Act, 2023 is India's first all-encompassing statute for the processing of digital personal data¹⁷. It's relevant to civil registration because information on civil registration is digitised and can be considered as personal data if it concerns an identifiable person. The Act should, however, be applied respecting the text and extent of the Act, and statutory exceptions.

It is not possible to state that all governmental processing operations are subject to the same treatment, or that the basis of consent is the only lawful basis for processing; the Act establishes grounds for additional lawful processing by public authorities: the processing is necessary for the performance of public functions which are entrusted to the public authority by law, and the processing is necessary for fulfilling a legal obligation¹⁸.

¹⁶ Rau's IAS, supra note 15.

¹⁷ The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), India Code.

¹⁸ Digital Personal Data Protection Act, 2023, § 7.

The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 are being brought into force through a three-phase commencement scheme. On 13 November 2025, MeitY issued four connected notifications, G.S.R. 843(E) to G.S.R. 846(E). Under G.S.R. 843(E), specified institutional and preliminary provisions of the Act came into force upon publication, while G.S.R. 844(E) established the Data Protection Board of India and G.S.R. 845(E) fixed its membership at four.

Correspondingly, Rules 1, 2 and 17 to 21 of the DPDP Rules, 2025 came into force upon publication under G.S.R. 846(E). The second phase commences one year after publication, calculated from the Gazette date as 13 November 2026, when section 6(9), section 27(1)(d) and Rule 4 concerning the registration and obligations of Consent Managers take effect. The third phase commences eighteen months after publication, calculated as 13 May 2027, when the principal substantive provisions governing processing, notice, consent, Data Fiduciary obligations, Data Principal rights, security safeguards and related matters, together with Rules 3, 5 to 16, 22 and 23, come into force.

Accordingly, as of September 2026, the DPDP framework remains only partially operational and should not be described as imposing all substantive obligations simultaneously. Reports that MeitY was considering compressing parts of the eighteen-month compliance period had not, by the paper's September 2026 cut-off, resulted in an amending instrument; meanwhile, constitutional challenges concerning the DPDP Act's amendment to the Right to Information Act remained pending before the Supreme Court following notice issued in February 2026.

The principles of DPDP are most useful for civil-registration governance is not limited to the issue of consent. They cover the duties of notice and transparency, reasonable security safeguards, organizational responsibility, and the restrictions imposed by the legislation itself, such as the Government's right to exempt instrumentalities of the State from certain obligations for the 'sovereignty, security of the State, public order or the prevention of

offences'¹⁹. A key policy question that is explored in more detail in this paper is whether a foundational database of the State, like the Registration of Births and Deaths Act, should have rules that go beyond the general rules of the DPDP framework to specify access, sharing and accountability.

E. Information technology and cyber security

The framework of information technology and the Information Technology Act, 2000, that governs the electronic records and digital infrastructure related to civil registration still applies²⁰. But cyber security would never be simply a matter of state compliance. The centralized public database needs an institutional security governance program, including technical resilience, incident response, logging, access control, authentication and responsibility for unauthorized access.

No substantiated evidence of a civil-registration database being compromised is used in this paper when making the legal analysis; no such claim is unsupported in this context. For the moment a more general and more defensible claim suffices: if data is concentrated (by any method, whether because of the nature of the data or its use, the decisions have to be made by the few, or perhaps the one person) there is more at stake in a successful compromise and, therefore, more constitutional and institutional significance in multi-level security and institution accountability.

VI. CONSTITUTIONALITY AND SUPREME COURT PRECEDENT.

A. Privacy as a Fundamental Right

The right to privacy is not just a fundamental right guaranteed by the constitution of india but it is also a basic human right.

The nine-judge Bench in Justice K.S. Puttaswamy (Retd.) v. Union of India²¹ unanimously declared that the "right to privacy" in the Constitution is a part and parcel of right to life

¹⁹ Digital Personal Data Protection Act, 2023, § 17(2).

²⁰ The Information Technology Act, 2000 (Act No. 21 of 2000), India Code.

²¹ *Supra*, 4

and personal liberty guaranteed under article 21. The judgment found that privacy was part of the guarantees of liberty, dignity, and that privacy has multiple and overlapping aspects, bodily privacy, decisional privacy and informational privacy.²² The decision has significant direct implications for government databases, since it overturns the idea that personal data can be less significant simply because it's stored by the State.

Puttaswamy does not, at the same time, impose an absolute prohibition on the collection of government data. The right to privacy is not absolute. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, Chandrachud J., speaking for four judges, stated that an invasion of privacy must satisfy a three-fold requirement: legality, requiring the existence of law; need, defined in terms of a legitimate State aim; and proportionality, requiring a rational nexus between the object pursued and the means adopted.²³

The utility of Puttaswamy for civil registration is mainly because of the analytical approach, not because of the fact that it is a birth or a death record. For civil-registration governance, this three-fold constitutional requirement provides the threshold framework. The proportionality inquiry was subsequently developed more specifically in the Aadhaar judgment, where Sikri J., drawing upon *Modern Dental College & Research Centre v. State of M.P.*, applied a four-stage analysis examining whether the measure pursues a legitimate goal, is suitable or rationally connected to that goal, is necessary in the absence of an equally effective less restrictive alternative, and maintains an appropriate balance between the governmental objective and the impact upon the individual right.²⁴

²² Id. ¶¶ 3, 169-183 (Chandrachud, J.).

²³ Id. ¶¶ 310, 325 (Chandrachud, J.); id. ¶ 638 (Kaul, J.).

²⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶ 325 (Chandrachud, J., for Khehar, C.J., Agrawal, Nazeer & Chandrachud, JJ.) (India) (stating the three-fold requirements of legality, need based on a legitimate State aim, and proportionality); *K.S. Puttaswamy v. Union of India (Aadhaar-5J.)*, (2019) 1 SCC 1, ¶ 319 (Sikri, J.) (India) (setting out the four-stage proportionality analysis); *Modern Dental College & Research Centre v. State of M.P.*, (2016) 7 SCC 353, ¶¶ 60-64 (India).

In principle, these questions should be considered at every phase of the data life cycle on collection, when central storage, when access to data is provided to other departments, and when secondary use and not always at the time of registration.

B. Aadhaar Jurisprudence

K.S. Puttaswamy v. Union of India (Aadhaar-5J.) was a five-judge Bench which interpreted and upheld the constitutionality of the Aadhaar framework while carving out exceptions and restrictions to certain provisions of the Aadhaar Act, 2016, such as access to broad categories of law enforcement agencies without judicial oversight, and provisions allowing the sharing of Aadhaar data with private entities²⁵. The litigation provides a precedent which is strongly analogous to civil-registration databases, but not the same.

The judgment looked at a system in which population-scale information was handled, a statute of purpose was in place, there was authentication and the potential for misuse, and it required that the large-scale digital system be evaluated by its statutory design and protections, instead of sweeping claims that it is inherently good or inherently bad²⁶.

In the context of the present subject, Aadhaar jurisprudence permits to draw a distinction between legitimate goals of the State and unlimited informational capability. It does not render the need to establish the limits of access and use to a database redundant because of its public nature, but neither does the presence of privacy interests extinguish the need for an administrative mechanism by the State.

The institutional design under law is the constitutional task in both contexts; an insight directly applicable to the governance of the national birth-and-death database set up by the 2023 amendment.

C. Constructing databases for birth and death information.

²⁵ *Supra*, 5. , ¶¶ 415-482 (India) (majority opinion of Sikri, J.).

²⁶ *Id.* ¶¶ 314-348 (applying the proportionality standard to the Aadhaar authentication architecture).

Close attention is required to the nature of the particular governmental activity involved in the application of privacy doctrine to civil registration. The registration of births and deaths is based on a piece of legislation with clear and non-controversial public purposes. The constitutional issue is more pronounced the further away information moves from the context of the original registration.

Aggregation can be accomplished in a central repository. The new section 3A (5)²⁷ of the amended 1969 Act allows new connections between the civil-registration database and other key identity and welfare data sources. The effects of secondary use can be different than what was known by the person, or their family, when a birth or death was registered. One helpful analytical tool developed for the purposes of this paper is to differentiate between four layers of civil-registration data life-cycle.

First, mandatory registration of a vital event may be necessary for the statutory system as such.

Secondly, it may be essential to keep an official record to administer that system and issue certificates.

Thirdly, the exchange of data in the registration architecture such as with the State and national databases could be needed to coordinate data nationally and to provide accurate statistics.

Fourthly, if the information is to be used for further administrative purposes (e.g., to update a ration-card database under section 3A (5)), it is necessary to consider, separately, the statutory authority, necessity and safeguards for the purposes for which it is proposed to be used.

A uniform concept of 'registration' for all four layers of the constitution masks the differences that Puttaswamy²⁸ asks the courts, and the lawmakers, to recognize.

²⁷ *Supra*, 2

²⁸ *Supra*, 4

VII. COMPARATIVE DATA-GOVERNANCE MODELS

A. Estonia: Interoperability instead of simple data concentration

This is not to say that Estonia has completely dispensed with centralization or that its approach is easy to replicate in India, but it is interesting to note that Estonia's experience highlights the value of a unique architectural decision, one that prioritizes interoperability through controlled exchange over universal data centralization. The Estonian Information System Authority and the Estonian e-Governance Academy describe X-Road (so called *artistikalt* X-tee) as a technological and organization-level data exchange layer which has been operating since 2001 and currently serves several hundred public and private information systems, processing billions of transactions every year.²⁹

Instead of passing information via one central server or master database, X-Road is a frame of communication, where independent information systems communicate with each other directly and every organization has a so called 'security server', which encrypts, signs, authenticates and logs all incoming and outgoing information³⁰.

The conceptual value of X-Road in the context of this dissertation is not a technical value but the architectural one. Digital government can be structured around explicitly controlled exchanges between separately controlled information systems, rather than around the unconstrained replication of all information into a unified operational repository. The lesson for India is that administrative integration and physical concentration of data are not synonymous options.

A system based on purpose-specific requests between separately controlled databases can provide the coordination benefits that motivate centralisation without requiring unrestricted concentration of all information in a single master repository. The broader

²⁹ Estonian Information System Authority (RIA), Data Exchange Layer X-tee, <https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee> (last visited Sept. 13, 2026); e-Estonia, X-Road, <https://e-estonia.com/service/interoperability-services/x-road/> (last visited Sept. 13, 2026).

³⁰ e-Estonia, *supra* note 30 ("To ensure secure transfers, all outgoing data is digitally signed and encrypted, and all incoming data is authenticated and logged.").

principle that interoperability need not require centralised storage, when combined with cryptographic authentication and mandatory logging, can impose meaningful institutional constraints on casual, unauthorised or unrecorded access. This principle is directly relevant to the design choices available to the Registrar General of India under the 2023 Amendment.

B. The European Union: Purpose Limitation and Accountability

Civil status is not a single civil-registration system for all the Member States of the European Union; it is a matter of national competence. The importance of this work in this dissertation is mainly due to a data-governance framework contained in the General Data Protection Regulation (GDPR), which while not directly applicable in India, provided an advanced and widely used normative language to assess any governmental database³¹.

The GDPR principles do not only just promote the principles of lawfulness, fairness and transparency but it focuses on promoting the importance and purpose limitation, data minimization, accuracy; storage limitation; integrity and confidentiality and accountability which are highlighted in Article 5³². They are not just aspirational, but actually form the basis of the Regulation and of the obligations and duties of both private and public-sector data controllers throughout the Union.

The most salient lesson in this present study is to have the purpose tied to the legality at every stage and not just at the time of initial collection. Once a lawful initial collection has been made, it does not necessarily grant permission to all future uses. Under Article 5(1)(b) of the GDPR³³, the data collected shall be collected for specified, explicit and legitimate purposes and shall not be further processed in such a way it is not against the proposed purpose. Further, Article 5(1)(c)³⁴ of the GDPR highlights that the data to be processed

³¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

³² GDPR, *supra* note 34, art. 5.

³³ *Ibid*, art. 5(1)(b).

³⁴ *Ibid*, art. 5(1)(c).

shall be adequate, relevant and limited to what is necessary in relation to those purposes. Article 5(2)³⁵ on accountability also directs the focus from mere promises to compliance to the actual institutional accountability of the controller. These principles collectively promote a life-cycle perspective on governance just like what is proposed in part 6.3 above and can be meaningfully used as a normative checklist for testing any future rules over access to India's national birth and death database as provided in section 3A(5) of the amended 1969 Act³⁶.

C. United Kingdom: Statutory Gateways and Controlled Disclosure

The United Kingdom provides another example, one that is neither a national database nor a general data-protection regulation, but a set of statutory gateways in individual institutions. Civil registration of births and deaths in England and Wales dates from 1 July 1837, while the Births and Deaths Registration Act 1953 principally consolidated the existing statutory framework rather than originating the registration system. The General Register Office continues to hold civil-registration records for England and Wales. Since 1 July 2009, birth and death registration has also operated through electronic records alongside the statutory paper-register system, resulting in parallel paper and electronic processes.

The Data (Use and Access) Act 2025, which received Royal Assent on 19 June 2025, further modernises this framework. Part 4 amends the Births and Deaths Registration Act 1953 and the Registration Service Act 1953 so that registers may be maintained electronically without the duplication previously created by the continuing requirement to maintain corresponding paper registers. The reform therefore does not introduce electronic registration for the first time; rather, it provides the statutory basis for moving from the dual paper-and-electronic practice operating since 2009 towards an electronic register

³⁵ *Ibid*, art. 5(2).

³⁶ *Supra*, 2

without an equivalent paper-register requirement.³⁷ The reform was not brought fully into operation merely upon Royal Assent and requires implementing measures. In 2026, the Government laid the draft Registration of Births and Deaths (England and Wales) (Specified Requirements) Regulations 2026 under the new section 38B of the 1953 Act. The instrument specifies requirements intended to replace the traditional ‘wet-signature’ requirement when an electronic register is used. It was considered by a House of Commons Delegated Legislation Committee on 1 September 2026 and approved by the Commons on 2 September 2026, following earlier approval by the House of Lords; as of September 2026, Parliament recorded the draft affirmative procedure as concluded.³⁸

Separately, Part 5 of the Data (Use and Access) Act 2025 amends the United Kingdom’s data-protection and privacy framework, including the UK GDPR and the Data Protection Act 2018. Part 6 establishes the Information Commission as a body corporate, abolishes the office of the Information Commissioner and transfers the Commissioner’s functions to the new Commission. These reforms therefore modify the existing data-protection framework rather than replacing it.³⁹

In the United Kingdom it is the comparative experience that disclosure of civil-registration data is possible – and in a mature system likely – only through a number of specific and identifiable statutory gateways (defining the purpose, the authority that receives the disclosure and the fields of the data disclosed). The assumption is that the normal situation is that no government has a right to have every other arm of government have access to the data in its possession. The greater lesson for India is that technological

³⁷ Data (Use and Access) Act 2025, c. 18, pt. 4 (U.K.); *Data (Use and Access) Act 2025: Explanatory Notes*, ¶¶ 530–549 (U.K.); General Register Office, *The General Register Office Celebrates 175 Years of Civil Registration*, GOV.UK (confirming commencement of civil registration on July 1, 1837).

³⁸ Draft Registration of Births and Deaths (England and Wales) (Specified Requirements) Regulations 2026; UK Parliament, *Statutory Instruments: Registration of Births and Deaths (England and Wales) (Specified Requirements) Regulations 2026* (recording laying on June 2, 2026, House of Lords approval on July 13, 2026, Delegated Legislation Committee consideration on Sept. 1, 2026, and House of Commons approval on Sept. 2, 2026).

³⁹ Data (Use and Access) Act 2025, c. 18, **pt. 5** (U.K.); *id.* **pt. 6**; *Data (Use and Access) Act 2025: Explanatory Notes*, ¶¶ 551 et seq., 907–915 (U.K.).

modernization of civil registration, such as the 2023 amendment, should ideally go hand-in-hand with similar clarity about who is to have access to the data, on whose authority, and for what clearly stated purpose – a direction that section 3A (5)'s⁴⁰ requirement for Central Government approval points to but is not on its own text fully realized through published rules.

D. Comparative Synthesis

There are not so many "models" that can be transplanted: three comparative jurisdictions support different, complementary propositions. Estonia shows that interoperability does not mean indiscriminate centralization; and that there is a way of exchanging data that is controlled, logged, cryptographically authenticated, and not dependent on a single master repository for administrative coordination. While the GDPR does not impose an obligation on India, there exists a developed and internationally influential framework of governance principles in the shape of the European Union's, which can be easily applied as an evaluative framework.

In the United Kingdom, the ongoing relevance of institution specific legal gateways in the management and disclosure of civil-registration information is shown, and the fact that even a mature common-law jurisdiction has recently, and warily, turned the birth and death registers to full electronic content. These systems cannot be imported wholesale into India, because they are different from India in terms of their constitutional set up, size and federal character.

As a group they do not support the view that a capable digital State must necessarily be a State whose functioning should be based on unrestricted concentration of personal information, and they provide institutional terminology – controlled exchange, purpose limitation, statutory gateways – for the proposals for reform set out in Part 9 of this paper.

⁴⁰ *Supra*, 2

VIII. JUDICIAL AND LEGISLATIVE DEVELOPMENTS: A TIMELINE

The above developments can be aptly summarized as the evolution of the relationship between legislative modernisation of civil registration and constitutional privacy doctrine as a chronology. The national statutory framework for civil registration was first provided by the Registration of Births and Deaths Act, 1969, which was implemented for 50+ years by the State in a largely manual approach⁴¹. The K.S. Puttaswamy (2017) judgment laid a foundation of privacy, including informational privacy, as a fundamental right and the proportionality test for evaluating the practices of the State.⁴²

On 26 September 2018, the Supreme Court delivered its Constitution Bench judgment in the Aadhaar litigation, applying constitutional privacy and proportionality principles to a population-scale digital identity system. While substantially upholding the Aadhaar framework, the Court struck down section 33(2) of the Aadhaar Act in its then form and held section 57 unconstitutional to the extent that it permitted the use of Aadhaar by a body corporate or person pursuant to contract, thereby imposing important limits on disclosure and private-sector use of Aadhaar information.⁴³

The Registration of Births and Deaths (Amendment) Bill, 2023 was introduced in the Lok Sabha on 26 July 2023, passed by the Lok Sabha on 1 August 2023 and by the Rajya Sabha on 7 August 2023. It received Presidential assent on 11 August 2023 and, pursuant to the commencement notification dated 13 September 2023, came into force on 1 October 2023.⁴⁴ The Digital Personal Data Protection Act, 2023 became a law only recently

⁴¹ Registration of Births and Deaths Act, 1969, *Supra* note 1.

⁴² Puttaswamy, (2017) 10 SCC 1, *Supra* note 4.

⁴³ *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar)*, (2019) 1 SCC 1 (India) (decided Sept. 26, 2018) (striking down § 33(2) of the Aadhaar Act in its then form and invalidating § 57 to the extent that it permitted Aadhaar use pursuant to contract).

⁴⁴ *Registration of Births and Deaths (Amendment) Act, 2023*, No. 20 of 2023 (India); PRS Legislative Research, *The Registration of Births and Deaths (Amendment) Bill, 2023*; Office of the Registrar General, India, Ministry of Home Affairs, S.O. 4058(E), *Gazette of India, Extraordinary* (Sept. 13, 2023) (India).

providing India with a general statutory regulation for personal-data processing, including through instrumentalities of the State⁴⁵.

The general data-protection framework and the national civil-registration architecture developed on partly overlapping timelines. The DPDP commencement notification and Rules were published on 13 November 2025 and established a three-phase scheme: specified institutional and Board-related provisions took effect upon publication; the Consent Manager provisions are scheduled to commence one year later, in November 2026; and the principal substantive obligations are scheduled to commence eighteen months after publication, in May 2027. Accordingly, as of the paper's September 2026 cut-off, the DPDP framework remained only partially operational.⁴⁶

This sequencing is also significant analytically. The national civil-registration database and its statutory data-sharing gateway became operative in October 2023, whereas the detailed rules under the general data-protection framework were notified only in November 2025. This sequencing is significant because, for a substantial intervening period, the civil-registration architecture developed without a fully operational general data-protection compliance framework. For a significant period, therefore, India has not had a fully implemented sector-specific rules-based general data-protection compliance regime to guide access, sharing, and retention – a fact that strengthens the argument to be made later in this paper that sector-specific rules under the Registration of Births and Deaths Act are needed to govern access, sharing, and retention in the interim and beyond.

IX. INTEROPERABILITY: TOWARDS ACCOUNTABILITY

A. Digital State Capacity: Benefits and Limits

⁴⁵ Digital Personal Data Protection Act, 2023, *Supra*, 19

⁴⁶ Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), *Gazette of India, Extraordinary*, pt. II, sec. 3(i) (Nov. 13, 2025) (India); Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 1(2)– (4) (India).

Fragmentation can be minimised using centralised or interoperable civil-registration data. Where authorities have to confirm a birth or death, if there are reliable official records, this can minimize duplication of documents and routine in administrative processes, thereby enhancing the citizen experience and the efficiency of institutions; a digital system can also make statistical reporting timelier.

Accurate vital-event information has many public uses, including death registration, which helps to maintain population records and official statistics; birth registration that provides legal evidence for foundational personal facts and, as amended in 2023, will be used for a variety of public purposes.⁴⁷ Proper registration may also help with the development of demographic data of importance to public-health policy. These are real and tangible gains and good reason for further investment in robust digital civil-registration infrastructure.

But the problem with many digital-government discussions is that there's a central analytical error when it comes to integration – that more integration equals more central storage. A government can provide a better service delivery without creating an unconstrained master repository that can be accessed by all institutions that may want to use it, using common technical standards and controlled data exchange, as the Estonian government does with its X-Road.

Federated or interoperable models might leave Institutional boundaries intact, cryptographic authentication and transaction records, and give an authorised authority access to verified information when it is truly needed. That is, the technological decision is constitutionally significant because architecture can make the information more or less repurposable or accumulative, irrespective of the formal provisions of the statute.

To evaluate a proposed civil-registration data practice, this paper proposes an author-developed four-part State Capacity Test, adapted from the four-stage proportionality

⁴⁷ *Supra*, 16.

framework applied by Sikri J. in the Aadhaar judgment and derived from *Modern Dental College*:

1. Does the practice pursue a legitimate administrative objective and materially improve the accuracy, efficiency or legality of public administration?
2. Is the proposed form of centralisation or data sharing suitably connected to achieving that objective?
3. Could an equally effective but less intrusive architecture such as verification on request rather than bulk transfer achieve substantially the same result? And
4. Does the overall balance between administrative benefit and interference with informational privacy remain proportionate, taking into account safeguards such as role-based access, audit logging and independent oversight?⁴⁸

Centralization is not per se excluded by this test. It demands centralization and each time statutory sharing under s.3A(5) of the amended 1969 Act must be justified as a necessary and proportionate and not default way of doing things.

B. Privacy and Data-Governance Threats

Centralization poses the greatest threat regarding privacy because of the possibility of data aggregation. A single civil-registration record can provide some information; a large and interoperable database can, when combined with other information systems, provide patterns at the population level, especially when provided by section 3A(5) with a civil-registration bridge to the population register, the electoral roll and the ration-card database, and other databases that are notified.

The privacy relevance of information, therefore, becomes relational: the privacy meaning can differ significantly if the datasets are merged, even if no one dataset, on its own, has

⁴⁸ Cf. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶ 325 (Chandrachud, J.) (India); *K.S. Puttaswamy v. Union of India (Aadhaar-5J.)*, (2019) 1 SCC 1, ¶ 319 (Sikri, J.) (India); *Modern Dental College & Research Centre v. State of M.P.*, (2016) 7 SCC 353, ¶¶ 60–64 (India). The State Capacity Test proposed in this paper is an analytical adaptation of this proportionality framework and is not itself a test formulated by the Supreme Court.

an especially high privacy meaning. Centralization can also minimize the practical friction which often meant that local paper records were not accessible.

The second danger is "function creep. With the establishment of an accurate national civil-registration database, demand for access to institutions will probably grow over time for purposes of fraud detection, eligibility verification, identity management or administrative coordination with new welfare or benefit schemes. Some uses may be completely legitimate, but the danger lies in the implementation of new uses through administrative practice or notification under section 3A (5) without public consultation and without an independent assessment of need.

A third risk relates to the possibility of surveillance and profiling: birth and death registration is not a surveillance programme and the Civil Registration System is not analytically a surveillance programme. However, a large-scale information base can only enhance surveillance potential if access rights are wide and controls are lax, and the pertinent legal issue is not what the information base is called, but what it is capable of.

Another concern relates to cybersecurity. Although centralisation may improve administrative efficiency, concentration of large volumes of civil-registration data can increase the systemic consequences of a security breach: compromise of a limited local register ordinarily affects a narrower dataset, whereas compromise of a large central repository may expose information on a substantially greater scale.

Decentralization is not necessarily the solution in every case, but a multi-layered approach to security, including robust authentication, access controls, isolation of environments, real-time logging, incident response, and independent security monitoring under the DPDP Act 'reasonable security safeguards and the IT Act 2000 framework'⁴⁹. A fifth risk is errors and corrections: errors can easily be propagated across a digital system and may result in a local problem if the error occurs in a local file, but a shared error across interconnected systems – for example, a wrong date of birth from the

⁴⁹ Digital Personal Data Protection Act, 2023, § 8(5).

civil-registration database to the electoral roll or a ration-card database – can get much harder to track and correct. However, civil-registration governance must be seen as a part of Digital State Capacity and not only as a single grievance mechanism.

C. Findings and research gap

As seen above, there are several findings:

1. First, civil registration has a legitimate status and need, and an analysis of constitutionality should not start with an antagonistic attitude towards public recordkeeping in general.
2. Secondly, digitization has implications for the practical use of records as it can improve the ability to find them, scale them and potentially make them interoperable, without any change to the legal requirement to register a birth or death.
3. Thirdly, the national data architecture for registered births and deaths in 2023 has been made significantly stronger by a sharing gateway in its section 3A (5) – questions of downstream governance are now far more pressing than in the unamended 1969 Act.
4. Fourthly, Indian privacy jurisprudence offers a constitutional framework that is well positioned to adjudicate these systems, even though the Supreme Court has not directly tested the constitutionality of the specific national database architecture established by the amendment in 2023 that this paper focuses on. Puttaswamy is thus a constitutional baseline for this discussion, and Aadhaar an analogue on matters of pop-scale digital infrastructure neither can be mischaracterized as a direct mandate on the birth and death register.
5. Fifthly, the role of general data protection and sectoral governance are complementary and distinct. A basic database of births and deaths created by the government in 2023 (or subject to registration under the Registration of Births and Deaths Act itself or under the provisions of section 3A(5)) could have far-reaching rights and obligations across the economy, but it may also

need specific rules – again ideally under the Registration of Births and Deaths Act, or under the provisions of section 3A(5) – on what particular data elements can be accessed, by whom, for what purpose and subject to what obligations of retention and audit. Where the general DPDP framework does exist on paper, it is not followed by people, due to uncertainty about the specific details of each sector.

This paper fills a gap in the Indian legal literature and policy debate that is created at the nexus of three still largely distinct areas of legal scholarship and policy discussion in India. Aadhaar and targeted surveillance are common points of discussion in privacy debates in India, as is the overall DPDP framework. However, conversations about civil registration are typically centered on how much registration is happening, how it works or how it serves statistical needs, like the legislative and policy documents that follow the amendment made in 2023.

A broad constitutional-law focus is often missing from the digital-government scholarship, which is often concerned with service delivery and technical interoperability. Focusing particularly on the constitutional implications of transitioning from civil registration to a national digital data infrastructure, and on the difference established during this paper between centralisation as such and privacy-preserving and accountable interoperability, there is comparatively little sustained attention in this area.

This dissertation sheds light on that intersection. The gap, however, must be stated with some care: it is an identified gap of analysis in the particular bodies of materials which have been examined in this paper, and it does not necessarily mean that no scholarship whatsoever exists on any single aspect of the subject.

D. Towards Accountable Interoperability

The real issue in Indian law is not whether India needs a modern Civil Registration System, but what institutional design is constitutionally appropriate once civil-registration records become digitally searchable and capable of being linked with other

databases. Reliable civil registration is essential both to public administration and to individual legal recognition. The more difficult question is how such digital infrastructure should be designed and governed consistently with constitutional requirements of legality, necessity, proportionality and informational privacy.

A dichotomy of central and decentral is insufficient in addressing this question. An entirely disjointed system is capable of producing administrative nightmares, and mismatched records and service delivery obstacles precisely like the 2023 amendment was meant to prevent. However, a totally free central repository could be an excessive centralization of the informational power that Puttaswamy is concerned about.

The legal option is based on the comparative analysis in Part 7, which has been to break down three concepts which are often lumped together in discussions about Indian policy: standardization, interoperability and central storage. National standards for data fields, formats and data quality may be desirable, but not necessarily available for all data. Estonia's X-Road enables interoperability without unlimited copying of the entire dataset to all the requesting systems. Having central storage may be warranted for some purposes – such as the authoritative record of a birth or death – but not for the general convenience of an administrative database that is accessible by non-essential government-related functions.

This distinction helps to establish what can be termed accountable interoperability. In such a model, information flows between institutions only through known legal gateways, which are adequately implemented via published rules, for example in the context of section 3A(5). Access is purpose-specific, role based and logged, based on purpose limitation and data minimization principles of GDPR. Just as X-Road does, the system records who requested information, when it was requested, by whom and for what purpose of the institution.

The authorization and review process is more stringent for high-risk or exceptional access, mirroring the requirements the Supreme Court had for disclosure of Aadhaar to law enforcement agencies. This approach ensures accountability but does not necessarily

require sacrificing the administrative efficiency the 2023 amendment was seeking; it renders proportionality real by asking not just whether a national database is useful in an abstract sense but whether each individual type of access is necessary, and can be repeated as often as new departments and schemes want to use it.

The DPDP framework can play a useful role in this model, but cannot be relied on as an alternative to sectorial regulation of civil registration. A civil-registration statute can go into detail about the responsibilities of institutions – who has the authority to request data, when, for how long, with what restrictions, etc. – that a general personal-data statute, affecting the entire economy, can't easily accomplish. For these reasons, governance measures should be allocated according to the statutory powers conferred by the Registration of Births and Deaths Act, 1969.

State Governments may make rules under section 30, with the approval of the Central Government, while the Central Government and the Registrar General of India may develop Model Rules and guidance and exercise the approval and notification powers applicable to the national database under section 3(5).

These mechanisms can be used to provide greater clarity concerning access, retention, audit and downstream updating without incorrectly attributing a general rule-making power under section 30 to the Central Government. The goal should be to not become paralyzed; the purpose of accountable interoperability is to facilitate legitimate data sharing in a more confident way, precisely because the edges and protections of interoperability are clear beforehand.

X. FINDINGS AND RECOMMENDATIONS

Based on the above analysis, these recommendations are addressed to the authorities according to their respective statutory functions. State Governments are the primary rule-making authorities under section 30 of the Registration of Births and Deaths Act, 1969, subject to the approval of the Central Government. At the national level, the Central Government and the Registrar General of India retain important functions relating to the

national database, including approvals and notifications under section 3(5), development of Model Rules and guidance, and determinations under section 17(3)(h). The Data Protection Board of India also has a relevant role, within the scope of the Digital Personal Data Protection Act, 2023, in relation to compliance with that framework.

1. Adopt clear rules and published access conditions governing disclosures of civil-registration data. State Governments, through rules made under section 30 where appropriate, and the Central Government when exercising its approval and notification functions under section 3(5), should require identification of the receiving authority, legal basis, defined purpose, specific data fields, frequency of access and applicable retention conditions. General administrative convenience should not substitute for a specific statutory gateway.
2. Where possible, take into account federated or controlled interoperability. India should evaluate, on a database-by-database basis, if the civil-registration information for a given administrative goal needs to be maintained at the central level, or if it only needs to be replicated to the central level on demand for a specific fact.
3. Adopt role-based access controls and tamper-resistant audit trails. State rules and administrative arrangements governing State databases, together with conditions attached to national-level access approved under section 3(5), should apply the principle of least privilege. Each access to or disclosure of civil-registration data should generate an auditable record capable of subsequent administrative or judicial review.
4. Implement data minimisation on a transaction-specific basis. When approving or regulating access under section 3(5) at the national level, or section 4(6) at the State level, the competent Government should ensure that a receiving authority obtains only those fields of a civil-registration record that are necessary for the authorised purpose, rather than receiving the complete record as a matter of course. This approach is consistent with the comparative principle of data minimisation reflected in Article 5(1)(c) GDPR.

5. Explicit, documented restrictions against function creep are adopted. Before authorising a new category of secondary use, the competent authority should conduct and document an assessment of legality, necessity and proportionality. In particular, the Central Government should undertake such an assessment before notifying an additional national-level database under section 3(5)(h), while State Governments should apply comparable scrutiny when approving disclosures under section 4(6).
6. Run data-governance impact assessments prior to significant architectural changes. Purpose, data flows, alternatives, risks and remaining safeguards should be evaluated prior to implementation of new interoperability arrangements and/or any high-risk secondary use of the national database.
7. Develop an effective correction and propagation plan. Errors in civil-registration systems must be addressable by a readily available process, and if errors have been addressed and information is already replicated in another system as a result of section 3A (5), then a mechanism must be provided for the system to communicate with the authentic records located downstream without causing unnecessary copies to be made elsewhere.
8. Set different "rules" for retention and archival for different types of records within a specific sector, separating long-term retention appropriate to an original civil record from the retention of operational copies, transaction logs and any derivative or analytical datasets, which do not require indefinite retention on the same basis.
9. Implement independent oversight and security audits of national and State databases that are consistent with the requirement to implement reasonable-security-safeguards under section 8(5) of the DPDP Act, including legal and governance compliance review.
10. Publish transparency information that at a general level describes the responsible institutions, the types of authorized recipients pursuant to section 3A(5), the general purposes of sharing and the mechanisms available for redress and

correction without compromising confidentiality commensurate to the security sensitive nature of the technical detail.

11. Maintain viable human and “off-line” channels for registration and correction, and ensure that digitization of the Civil Registration System is not de facto making registration/correction unfeasible for persons impacted by connectivity, literacy or technological challenges.
12. Follow the principle of continuing constitutional review in the architecture of the databaseThe Central Government and State Governments should, within their respective statutory spheres, periodically review the legality, necessity, proportionality and safeguards applicable to new interoperability arrangements. At the national level, such review should accompany approvals and notifications under section 3(5); at the State level, it should accompany approvals under section 4(6) and relevant rules made under section 30.

XI. CONCLUSION

Centralization of birth and death records is an important constitutional issue in the digital State. A greater technological capacity can indeed enable civil registration and improved national coordination, but it does not warrant more governmental control of the personal information.

Civil registration data is required by law, but does not necessarily imply the collection of it in an unrestricted way, for aggregation, for sharing or for secondary use. The State action that impinges into privacy needs to meet the tests of legality, legitimate state purpose, proportionality and effective safeguards, as recognized in *Puttaswamy*. The Aadhaar jurisprudence exemplifies the need to be wary of digital infrastructure operating at a scale that affects the population.

The European Union and the United Kingdom have experienced the effectiveness of digital governance that integrates interoperability with measures like purpose limitation, controlled access, and accountability measures.

India should thus opt for accountable interoperability and not data concentration. It is very pertinent and salient to understand the importance of having the clarity of legal purposes, role-based access, audit trails, data minimization, security measures and independent human oversight and absence of which it is impossible to ensure that civil-registration infrastructure does not reduce constitutional rights but enhances State capacity.

XII. BIBLIOGRAPHY

A. Constitutional and Statutory Materials

1. The Constitution of India, sch. VII, list III, entry 30.
2. The Registration of Births and Deaths Act, 1969 (Act No. 18 of 1969), India Code.
3. The Registration of Births and Deaths (Amendment) Act, 2023 (Act No. 20 of 2023), India Code.
4. The Registration of Births and Deaths (Amendment) Bill, 2023, Bill No. 93 of 2023 (as introduced in Lok Sabha, July 26, 2023).
5. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), India Code.
6. Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025, Gazette Notification No. G.S.R. 846(E) (Nov. 13, 2025).
7. The Information Technology Act, 2000 (Act No. 21 of 2000), India Code.
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
9. United Kingdom, Data (Use and Access) Act 2025, c. 18.
10. United Kingdom, Births and Deaths Registration Act 1953, as amended by the Data (Use and Access) Act 2025.

B. Cases

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
2. K.S. Puttaswamy v. Union of India (Aadhaar-5J.), (2019) 1 SCC 1 (India).

C. Official Government and Institutional Sources

1. India Code, Ministry of Law and Justice, Government of India, Registration of Births and Deaths Act, 1969, <https://www.indiacode.nic.in>.
2. PRS Legislative Research, The Registration of Births and Deaths (Amendment) Bill, 2023, <https://prsindia.org/billtrack/the-registration-of-births-and-deaths-amendment-bill-2023> (last visited Sept. 13, 2026).
3. Rau's IAS, The Registration of Births and Deaths (Amendment) Act, 2023, <https://compass.rauias.com/current-affairs/registration-births-deaths-amendment-act-2023/> (last visited Sept. 13, 2026).
4. IMPRI Impact and Policy Research Institute, Registration of Births and Deaths (Amendment) Act, 2023, <https://www.impriindia.com/insights/birth-death-act/> (last visited Sept. 13, 2026).
5. S.S. Rana & Co., MeitY Notifies Final Digital Personal Data Protection Rules 2025, <https://ssrana.in/articles/meity-notifies-final-digital-personal-data-protection-rules-2025/> (last visited Sept. 13, 2026).
6. Shardul Amarchand Mangaldas & Co, Enforcement of the DPDP Act and Notification of the DPDP Rules, <https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/> (last visited Sept. 13, 2026).
7. Khurana & Khurana, MeitY Notifies Rules Operationalising the DPDP Framework, <https://www.khuranaandkhurana.com/update-meity-notifies-rules-operationalising-the-dpdp-framework-in-india> (last visited Sept. 13, 2026).
8. EUR-Lex, Regulation (EU) 2016/679, Article 5, <https://eur-lex.europa.eu>.
9. Estonian Information System Authority (RIA), Data Exchange Layer X-tee, <https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee> (last visited Sept. 13, 2026).
10. e-Estonia, X-Road, <https://e-estonia.com/service/interoperability-services/x-road/> (last visited Sept. 13, 2026).

11. UK Government, Data (Use and Access) Act 2025, <https://www.legislation.gov.uk/ukpga/2025/18> (last visited Sept. 13, 2026).
12. Hunton Andrews Kurth, UK Government Publishes Commencement Dates for the UK Data (Use and Access) Act, <https://www.hunton.com/privacy-and-information-security-law/uk-government-publishes-commencement-dates-for-the-uk-data-use-and-access-act> (last visited Sept. 13, 2026).
13. LegalClarity, Data Use and Access Act 2025: Key Changes Explained, <https://legalclarity.org/data-use-and-access-act-2025-key-changes-explained/> (last visited Sept. 13, 2026).