FROM TITLE TO DATA: RECONCILING THE TRANSFER OF PROPERTY ACT, 1882 WITH THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND DIGITAL PERSONAL DATA PROTECTION RULES, 2025 IN KARNATAKA'S E-GOVERNED LAND ECOSYSTEM

Sunandeni R, Advocate, Bangalore

Shivanshi Mishra, Hidayatullah National Law University

ABSTRACT

The digitisation of land records does not simply affect the way in which land is transferred, but the way in which the people behind the land become visible to the State, markets and each other. All of this is becoming more apparent in Karnataka with its ever-closer land platforms. This article explores the interplay between the Transfer of Property Act, 1882, the Digital Personal Data Protection Act, 2023 and its 2025 rules, and the evolving registration framework. It then addresses the continuity of substantive property law through doctrinal analysis of statutory provisions, constitutional privacy jurisprudence and recent judicial decisions, suggesting that this continuity is accompanied by a re-distribution of transactional risk across public databases and private intermediaries. A public-record paradox is central to this inquiry: information disclosed under the law to secure reliability of title may fall outside statutory data-protection safeguards, but at the same time the digitisation of information means that it can be aggregated, profiled and commercially re-used in ways never imagined by the lawmakers. The article further identifies the disconnect between the responsibilities for data accuracy and the rights of individuals to correct the data, between the digital verification and the meaningful procedural review, and between the responsibility for data breaches and remedies for the proprietary effects of the breach. It advocates for a governance framework based on proportionate public access, correction through interdependent systems, human consideration of digital objections, accountable vendor relationships and coordinated incident response. Its central claim is that informational privacy is integral to reliable digital land administration: the security of property rights increasingly depends on the governance of the data through which those rights are recorded, verified and exercised.

1. Introduction

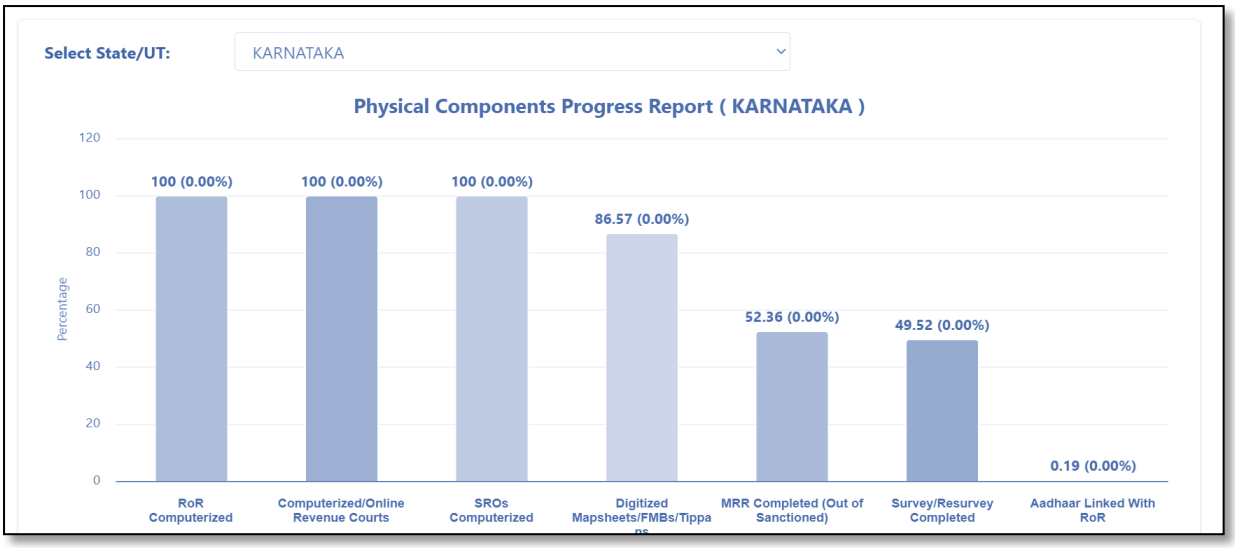
The digitisation of platforms such as Bhoomi, Kaveri 2.0, E-swathu/E-asthi (Bruhat Bengaluru Mahanagara Palike), /E-asthi (Karnataka)/ GIS Property Identification Numbers, FRUITS database, RERA online filings and KIADB digital land allotment portals have changed the overview of land administration in Karnataka and have transformed the legal architecture of immovable property transactions.

While proprietary rights continue to be governed by the Transfer of Property Act, 1882 (**TPA**), the execution, verification, evidence and security of such transactions increasingly depend on personal-data-driven platforms. With the enforcement of the Digital Personal Data Protection Act, 2023 (**DPDP Act**) and Digital Personal Data Protection Rules, 2025 (**DPDP Rules**) Karnataka now sits at the intersection of property law and data protection law, introducing fresh liabilities and compliance duties across recording authorities, banks, developers, sub-registrar offices, and land-technology intermediaries.

This article examines the doctrinal continuity of the TPA alongside Karnataka's evolving data-risk landscape within land governance, highlighting regulatory gaps, case-based insights, and a policy roadmap to synchronise property rights with informational privacy.

Karnataka has been recognised as a leader in land-record digitisation, ranking among the top states under the Digital India Land Records Modernisation Programme (DILRMP)[1]. The State achieved 100% digitisation of Record of Rights, Tenancy and Crops (RTC) and mutation registers through Bhoomi, and over 90% of property registrations shifted to Kaveri 2.0 by 2024.

[1] *Digital India Land Records Modernization Programme—MIS 4.0 Dashboard*, Department of Land Resources, https://dilrmp.gov.in/dashboard-chart.



The E-Khata system, GIS-based Property Identification Numbers, RERA Karnataka, the FRUITS database for farmers, and KIADB's land-allotment portals now form a consolidated digital ecosystem that stores and processes large volumes of individually identifiable information.

While the TPA continues to govern alienation of immovable property, it never contemplated a scenario in which transfer documentation, title history, identity verification and payment trail would rely heavily on personal data. The DPDP Act, 2023 fundamentally reconfigures this landscape by imposing consent-based, purpose-limited, and security-mandated processing of personal data arising from property transactions. As a result, modern land transactions involve dual compliance: TPA requirements for proprietary rights, and DPDP requirements for informational privacy.

2. Doctrinal Stability of TPA in a Digitised World

The TPA's scheme remains the backbone of immovable property transactions.

- Section 5 defines transfer by act of parties, and now the documents are electronically uploaded and registered in the Office of the Sub-Registrar, digitally traceable consideration.

- Section 53-A (part performance) becomes capable of specific performance on timestamped digital Agreements to Sell.

- Section 54 mandates registered instruments for sales of immovable property.
- Section 55 imposes duties on sellers and buyers, with "disclosure of material defects" increasingly interpreted in practice to include digital encumbrances and litigation data.
- Section 60 (redemption) now implicates digitally issued mortgage-release certificates.

Judicial interpretation confirms the enduring primacy of TPA over transfer of rights, but accepts digitised evidence for adjudication. In *Suraj Lamp & Industries v. State of Haryana*[2], the Supreme Court held that transfer of immovable property cannot occur through GPA, affirming the requirement of a registered Sale Deed, a principle applied uniformly even in digital execution environments.

Thus, digitisation has modernised the evidentiary pathway but not weakened the proprietary scheme of the TPA.

3. DPDP Act[3] & DPDP Rules[4] 2025 — New Compliance Layer for Property Transactions

The DPDP Act[5] introduces a rights-based framework for processing personal data. Key provisions relevant to land and real estate include:

- Section 3 — Consent for processing personal data
- Section 6 — Notice to the Data Principal
- Section 7 — Legitimate uses for KYC in registration and lending
- Section 8 — Duties of Data Fiduciaries
- Section 9 — Children's data
- Section 16 — Reporting of breaches
- Schedule — Penalties up to ₹250 crores.

[2] Suraj Lamp & Industries (P) Ltd. v. State of Haryana, (2012) 1 SCC 656 (India).
[3] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[4] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India).
[5] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

The DPDP Rules 2025[6] introduce sector-agnostic obligations including:

- Encryption of personal data in transit and at rest
- Periodic deletion
- Breach logging
- Consent records
- Data minimisation
- Vendor oversight

In Karnataka, real-estate platforms, developers, banks, sub-registrars and aggregators become Data Fiduciaries, while buyers, sellers and tenants are Data Principals and third party service providers such as CRM platforms and document management systems or verification agencies become Data Processor.

The notification of the DPDP Rules, 2025 and the progressive implementation of the Act on 13 November 2025 introduces valuable temporal aspects to this compliance regime. The provisions of the Act, including the establishment of the Data Protection Board of India ("DPBI") under Section 18-26, took effect immediately. Existing substantive provisions, such as grounds for processing, consent framework, some legitimate uses, Data Fiduciary obligations, and rights of Data Principals are scheduled to take effect eighteen months after notification. The Rules are staggered in a similar manner: Rules 1, 2 and 17–21 came into force upon publication; Rule 4 follows after one year; and Rules 3, 5–16, 22 and 23 after eighteen months.[7]

This gradual rollout is crucial to the digital land ecosystem in Karnataka. The substantive requirements that will apply to the processing of personal data (such as notice requirements, checking of accuracy, security measures and procedures on data breaches) some of which already apply to the processing of personal data at scale on the platforms such as Kaveri 2.0

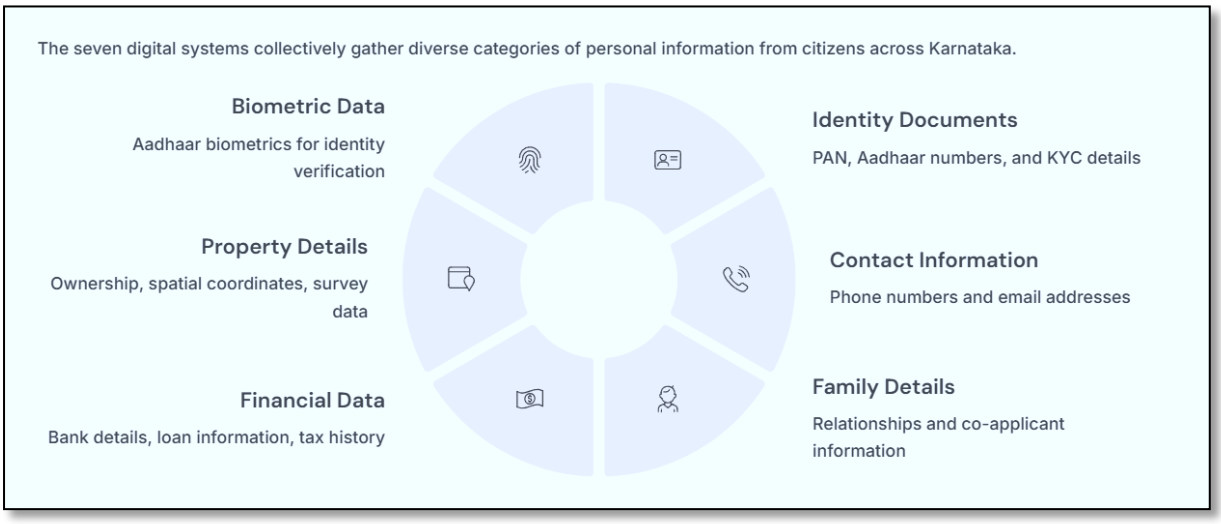
[6] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India).
[7] Ministry of Electronics & Information Technology, Notification G.S.R. 843(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India); Digital Personal Data Protection Rules, 2025, r. 1, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India).

and Bhoomi, will only come in force at the end of the transition period. The present interval is thus not one of deferred compliance, but provides a window within which the current land administration system can be examined and restructured prior to the coming into effect of the substantive regime.

The institutional framework is itself still developing. Although the DPBI has been formally established, MeitY invited applications for one Chairperson and four Members in May 2026.[8] The design decisions being engrained into the platforms of the State of Karnataka are particularly consequential, given that the DPBI remains in an incomplete form, despite being formally established, and that the data-protection framework is currently in a phase of implementation.

4. Karnataka's Digital Land Ecosystem: Interface with DPDP

The process flow of personal data is critical during property transactions and below listed types of personal data collected on various platforms



DPDP introduces additional liabilities for each of these systems, including breach reporting and deletion governance.

The digital land ecosystem of Karnataka is becoming more and more interoperable, with less reliance on siloed databases. Kaveri 2.0 acts as a central registration interface that fetches

[8] Ministry of Electronics & Information Technology, *Appointment to the Post of Chairperson and Other Members in the Data Protection Board of India*, F. No. 2(1)/2026-Pers.I (May 6, 2026).

property information from various databases such as Bhoomi, e-Swathu, e-Aasthi, and its broader ecosystem connects with the identity verification, payment, survey data, agricultural records, and digital documentation services. The Department of Stamps and Registration itself records that property details are pulled from Bhoomi, e-Swathu and e-Aasthi; registration can be given a digital mutation; party names and area information can be checked against the land records before registration.[9] Thus, the information originally maintained in different administrative systems, can find itself in a common transactional workflow.

This interoperability may then generate a significant level of administrative efficiency but also the danger of function creep: data gathered and stored for one set of administrative functions may then be used for another function in a different administrative system or decision-making process. For example, revenue and municipal records can be inputs in registration, identity information can be utilized for party validation, and information contained within registration can be utilized for mutation processes. The worry is not only the amount of personal information gathered in the course of a real estate deal, but also the increased potential of the existing dataset to be technically utilized.

The DPDP Act does not explicitly forbid this interoperability and does not provide consent as the only basis of law for these data flows. Section 4 permits processing for a lawful purpose on the basis of consent or the "certain legitimate uses" enumerated in Section 7. In particular, Section 7 recognises specified forms of processing by the State and its instrumentalities, including processing for the performance of functions under law.[10] Interoperability is not, however, an independent legal basis for processing. As the substantive provisions of the DPDP framework come into effect, the legal basis and purpose of each material flow of personal data across interconnected systems will therefore be in focus, instead of being assumed from technical integration alone.

This separation is particularly relevant because the state of Karnataka is furthering the integration of its land governance infrastructure. The State's Economic survey of 2025-26 talks about an Integrated Land Management System with the departments such as Urban Development, Rural Development & Panchayat Raj, Housing, BDA, BMRDA and KIADB, with digitisation of property transactions & permissions, and integration of e-Khata with Kaveri

[9] Department of Stamps & Registration, Government of Karnataka, KAVERI 2.0: Karnataka Valuation and e-Registration Initiative 7, 19 (Sept. 12, 2024).
[10] Digital Personal Data Protection Act, 2023, §§ 4, 7, No. 22, Acts of Parliament, 2023 (India).

2.0.[11] As these systems become more interoperable, the regulatory question is not whether digitisation is allowed or not, but how data shared across different statutory functions can be reused, shared and governed without the administrative convenience becoming a license to secondary use.

5. Legal Conflicts — TPA vs DPDP in the Karnataka Context

Context	TPA Position	DPDP Position
Proof of identity for sale	Silent	Requires consent & deletion
Storage of past title documents	Permissible	Not permissible beyond purpose
Sharing buyer data with brokers	Not regulated	Illegal without consent
Payment trail	Evidence	Financial data becomes protected personal data
Retention of KYC	Not governed	Strict deletion mandated post-purpose

Thus, a land transfer may be valid under TPA but illegal under DPDP if personal data compliance fails.

5.1 The Public-Record Paradox: Statutory Publicity Meets Informational Privacy

Land-registration law is premised upon publicity. The public nature of the books and indexes is necessary to a proprietary function which was recognized in section 57 of the Registration Act, 1908, which makes it expedient that they be open for inspection, and that copies of the entries be made available on payment of a fee.[12] But the DPDP Act has a quirk that is unique to digitised public records. Section 3(c)(ii) of the DPDP Act, when in force, removes from the scope of the Act personal data made publicly available by the Data Principal or by another person who has a legal obligation to make it publicly available.[13] Land records that are required by law to be made public may, therefore, fall outside of the scope of the DPDP Act despite

[11] Government of Karnataka, Economic Survey of Karnataka 2025–26 (2026).
[12] Registration Act, 1908, § 57, No. 16, Acts of Parliament, 1908 (India).
[13] Digital Personal Data Protection Act, 2023, § 3(c)(ii), No. 22, Acts of Parliament, 2023 (India).

their digitisation substantially increasing the risk of privacy.

A. Compulsory Disclosure and the Limits of the Public-Data Exclusion

This omission fuels a conflict between the purpose for which a piece of information ought to be public and the implications that stem from its online presence. A landowner's furnishing of identity and transactional information for registration is based on the requirement of the law that the identity and transactional information be publicly recognized and published upon registration; this is different from an individual's voluntary placement of the same information in the public domain. The Aadhaar litigation makes it clear that compulsion is intrinsically linked to the constitutional meaning of collection and use of personal information: The Supreme Court in the case held that the collection, aggregation and dissemination of personal information data by the State is a fundamental violation of information privacy and can only be done within the constitutional framework of legality and proportionality.[14]

However, Section 3(c)(ii) does not explicitly consider whether the personal data is voluntarily published or information becomes public when another person is legally compelled to publish it; it expressly contemplates both categories. The question is not then whether statutory land records should continue to be publicly available but whether the mandatory publicity of the records, as a result of the requirement, should exempt the resulting digital dataset from standard data-protection protections completely. In the land context, the difference between publicity necessary to establish and investigate title and complete unrestricted information about the individuals behind the title becomes significant.

B. Analog Publicity Is Not Digital Ubiquity

It does not mean, however, that privacy implications of a record remain the same when it is digitized and made “public.” Historically, access under the Registration Act was limited to those who wanted to have it inspected or access copies of it via the registration system, subject to the statutory process and prescribed fee. These practical constraints can be significantly diminished by the application of digitisation: with current technology, the site information can be retrieved, searched, cross-referenced and extracted or aggregated remotely, to a scale which could not be practically achieved by physical inspection. The information is the same, but its

[14] K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 (India).

practical accessibility has significantly changed.

This is important as property records can provide much more than just the existence of a title. When transaction histories, the names of the parties, consideration, encumbrances, mortgage interests and identifiers related to transactions become capable of being linked across datasets, they can allow for inferences about someone's assets, financial relationships and transaction history. The Supreme Court's informational-privacy jurisprudence acknowledges that there can be privacy issues that arise from the aggregation and disclosure of information even when legitimate privacy interests in transparency coexist. For example, in Association for Democratic Reforms v. Union of India, the Court recognised the existence of financial contributions which could engage informational privacy but also struck a balance between the requirement of disclosure and the demands of constitutionally protected informational privacy. In the context of land records, this is also a point that is relevant: publicity and privacy are not mutually exclusive; and the extent and the structure of disclosure are matters.

C. Scraping, Aggregation and the Regulatory Gap

The generated availability of public records raises a second question about downstream use. Commercial entities such as property portals, data brokers, title-search providers, or others who may be technically able to gather publicly available land information, process it with information from other sources, and create searchable land ownership histories or profiles. This is qualitatively different from the State keeping a registry to enable a purchaser to investigate title.

However, the DPDP Act is not as clear as it may first appear about resolving this issue. Without additional legislative or judicial guidance, it would be hard to imagine that all subsequent commercial processors of personal data are bound by the DPDP Act simply because they have other purposes for the data than the one for which it was originally publicly disclosed. This leaves a potential regulatory gap, since the very access that is necessary to complete property transactions may lead to aggregation and profiling that is not covered by the DPDP framework.

The proper reconciliation is not to obliterate or cover up the historical record upon which title is based. Instead, Karnataka's digital land architecture should differentiate between the legal publicity of the land title and its technical architecture, through which the information is made public. The bulk extraction, automated scraping, cross-database aggregation, commercial reuse

of individual inspection and legitimate title search may not be considered technologically the same, just because they come from the same public record. This difference is the foundation for access control and privacy-by-design approaches that maintain a reliable and public land record, while not transforming statutory publicity into digital legibility.

6. Navigating through intersection of DPDP Act, DPDP Rules with Registration (Karnataka Amendment) Act, 2023[15] and the Karnataka Registration (Refusal and Cancellation of Registered Documents) Rules, 2025[16] (Registration Rules 2025):

The Registration Act of 2023 introduced five critical new sections that fundamentally transform Karnataka's property registration system which includes:

I. **Section 22-B: Power to Refuse Registration:** Registrar must refuse registration of forged documents, documents prohibited by any Central or State Act, transactions relating to attached immovable properties, and any other category notified by the State Government.

II. **Section 22-C: Cancellation of Registered Documents:** District Registrar can cancel registrations (suo motu or on complaint) if they violate Section 22-B. Notice must be issued to all affected parties and subsequent purchasers.

III. **Section 22-D: Appeal Mechanism i.e.,** Appeal lies before Inspector General of Registration (IGR) against cancellation orders, ensuring judicial oversight.

IV. **Section 81-A: Penalty for Officers,** registering officer registering forged or prohibited documents faces up to 3 years imprisonment, fine, or both, except where done in good faith.

V. **Section 81-B: Offences by Companies:** Directors, managers, and officers are liable unless they prove lack of knowledge or due diligence.

Draft Registration Rules 2025

The Rules give operational structure to Sections 22-B to 22-D, establishing practical

[15] Registration (Karnataka Amendment) Act, 2023, No. 47, Acts of Karnataka State Legislature, 2024 (India).
[16] Karnataka Registration (Refusal and Cancellation of Registered Documents) Rules, 2025 (India).

mechanisms for implementation and enforcement. In terms of the said Rules, a document may be refused based on the following:

I. Forged Documents Registration can be refused if document appears forged or electronic database fails to confirm authenticity through integrated systems;

II. Identity Verification that is when authenticity of executing parties' identity cannot be verified based on prescribed Identity Documents;

III. Prohibited Transactions* Documents relating to transactions prohibited by Central or State Acts as notified in Official Gazette;

IV. Attached Properties* Transfer of immovable property subject to permanent or provisional attachment orders from Courts, Tribunals or Competent Authorities.

* A new integrated electronic Register of Prohibited Transactions will be maintained by IGR for real-time verification, and a Register of Attachments will ensure no transfer can be registered until orders are vacated or stayed.

Thus, Karnataka Registration Amendment read with Draft Rules 2025 expands the Sub-Registrar's powers to refuse registration where documents appear forged or identity cannot be verified, and to cancel registrations (suo motu or on complaint), and if later integrated database checks or investigation reveal fraud. It also mandates cross-verification against integrated electronic databases and expands compulsory registration categories (e.g., POAs). This materially raises post-registration exposure for the purchaser perspective.

Thereby, property documents are now at a point of dual legal risk — (a) regulatory / penal / remedial risk under DPDP for mishandling *Personally Identifiable Information* (**PII**), and (b) cancellation/invalidity risk under Registration Rules where document authenticity or identity verification fail. Both can arise from the same conduct (e.g., sloppy e-KYC or vendor failures).

6.1 Data Accuracy as a Property-Rights Concern

In addition to this dual-risk framework, the growing use of integrated databases adds one more problem area relating to data quality and the accuracy of the information on which registration and mutation decisions depend. In the context of a digital land-registration system, ensuring

the completeness, accuracy and consistency of the data held by a Data Fiduciary becomes important not only for informational privacy, but also for the accuracy of data. A wrong ownership entry or survey identifier, an incorrect attachment status, or a property record can impact whether or not a transaction can proceed.

This connection is of particular significance with reference to the Registration Rules, 2025. They allow refusal when an integrated electronic database fails to confirm the authenticity of the document,[17] and consider refusal when properties or transactions are not retrievable from, verified against or matched with a notified departmental database or software.[18] The reliability of the underlying database becomes capable of affecting the exercise of proprietary rights. Although a system of registration may be technically correct, it may still yield a wrong result when the authoritative data that it uses to register a transaction is incomplete, out-of-date or fails to accurately portray the legal situation.

This is not hypothetical, as the Karnataka High Court has recently ruled in favour of Karnataka government in a number of instances. In Gilbert Vas v. State of Karnataka, the Court held that Kaveri 2.0 did not have a specific workflow to facilitate the issue of mutation for civil court decrees and that this meant that revenue records could continue to show superseding ownership even after final orders by the judiciary. In B. Shivanna v. State of Karnataka, the Court had also noted that there was a "systemic incongruity" because of the insistence on e-khata which was capable of preventing execution of a decree for specific performance, hence, it had ordered to issue e-khata and to register the court-executed sale deed.

The decisions are indicative of a bigger issue. For an interoperable system, the impact of the inaccurately recorded, incomplete or structurally inadequate record is not only limited to the database in which it was created. If a mistake or omission occurs in one layer, a legal transaction might not work through another layer. Data quality thus becomes a data protection matter and a property administration matter at the same time.

This issue is only partially addressed by the DPDP Act. Section 8(3) imposes an accuracy obligation where the statutory conditions are satisfied. However, the individual right to correction under Section 12 is framed more narrowly, applying to personal data processed on

[17] Karnataka Registration (Refusal and Cancellation of Registered Documents) Rules, 2025, r. 3(2) (India).
[18] *Id.* r. 6(2)(a).

the basis of the Data Principal's prior consent, including consent under Section 7(a).[19] State processing of land data may, depending on its statutory basis, instead fall within other limbs of Section 7. A general accuracy obligation, therefore, does not automatically lead to a general individual correction mechanism for all inaccuracies in the government's land databases. In the land context, what is needed is an integrated correction architecture that can trace back an incorrect datum back to its source and correct that datum throughout all of the interconnected registration, revenue and municipal systems that depend upon it.

6.2 Digital Refusal and Procedural Fairness

The same structure poses a unique question of procedural justice. Database verification is explicitly included as a statutory ground of refusal in the Registration Rules, 2025. A document may be refused where an integrated database fails to confirm its authenticity, where the identity of executing parties cannot be verified through prescribed documents, or where property or transaction particulars fail to match a notified departmental database.[20] The Rules thus allow digital systems to be important inputs to the decision of whether a document should enter the registration system at all.

But to say the present system is one of "automated refusal without human adjudication" would be an exaggeration. The final Rules require the Registering Officer to record reasons for refusal, provide a copy of those reasons to the affected person, and provide an appellate route.[21] The more pertinent question is whether these safeguards are meaningful when the immediate reason for refusal is also a consequence of the work of another digital system upstreamA Sub-Registrar may be capable of explaining that Kaveri 2.0 cannot verify or match a record without necessarily possessing the authority or technical capacity to correct the source database responsible for the mismatch.

Karnataka's recent jurisprudence illustrates the difference between a legal entitlement and its digital implementation. In V. Prasad v. State of Karnataka, the High Court had to deal with a Kaveri–e-Swathu integrated system that automatically rejected documents where software prerequisites were not satisfied, and directed that the software be brought into conformity with the Registration Act and Karnataka Registration Rules. The Court's underlying proposition was

[19] Gilbert Vas v. State of Karnataka, W.P. No. 26357 of 2024, 2025:KHC:47151 (Karn. H.C. Nov. 14, 2025) (India).
[20] Karnataka Registration (Refusal and Cancellation of Registered Documents) Rules, 2025, rr. 3, 6 (India).
[21] *Id.* rr. 7–8.

that deficiencies in software architecture cannot add conditions inconsistent with the governing statute. In a recent case, Sunil Mahadev Athanikar v. Panchayat Development Officer, an applicant for e-Swathu had received an endorsement referring only to a "technical issue" when the procedure provided for an online application. The Court emphasized the need for State authorities to communicate clearly and transparently when a digital-only procedure is required.[22]

The constitutional importance of these safeguards is strengthened by Article 300A. While the case of Kolkata Municipal Corporation v Bimal Kumar Shah was concerned with the compulsory acquisition of property, the requirements in that case cannot be mechanically applied to all registration proceedings. The more general idea that State interference with property should be organised through a legally authorised and meaningful process does offer a good constitutional yardstick for digital land administration.

The absence of human review isn't the regulatory gap, however. There are safeguards and reasons already provided in the Registration Rules of Karnataka. The unresolved issue is fragmented review, that is, whenever a refusal is issued due to an incongruency in Bhoomi, e-khata, e-Swathu or any other integrated database, a challenge to the Sub-Registrar's refusal will not necessarily rectify the upstream record that caused the refusal. Procedural fairness in an interoperable registry then demands that there be a mechanism to trace back to the origin of the digital objection, to challenge the data upon which it is based, to correct the data if it is inaccurate, and to share that correction throughout the interoperable systems. A statutory right of appeal that does not tackle the cause of a data error may address only the consequences of that error.

7. Privacy Rights and the Constitutional Dimension

The constitutional structure that regulates such data processing was developed through the two decisions in Justice K.S. Puttaswamy (Retd.) v. Union of India. In 2017, a nine-judge Bench of the Supreme Court unanimously affirmed privacy as a fundamental right protected under Part III of the Constitution. The subsequent Aadhaar judgment in 2018 upheld the use of Aadhaar for specified statutory purposes, while striking down the part of Section 57 of the

[22] Sunil Mahadev Athanikar v. Panchayat Development Officer, W.P. No. 100979 of 2026, 2026:KHC-D:2636, ¶¶ 10–12 (Karn. H.C. Feb. 19, 2026) (India).

Aadhaar Act that enabled private entities to use Aadhaar pursuant to contract.

The scheme faced its constitutional test in *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017/2018),* where the Supreme Court affirmed privacy as a fundamental right under Articles 14, 19, and 21. The judgment upheld Aadhaar's validity for welfare delivery under Section 7 of the Aadhaar Act, but curtailed private-sector use by reading down Section 57 of the Aadhaar Act. It also imposed strict privacy safeguards—such as data minimization, limited retention, authentication protocols, siloed data storage, and yes/no responses from the Central Identities Data Repository (CIDR).

The importance of this jurisprudence goes beyond the use of Aadhaar itself. Puttaswamy establishes that State processing of personal information is subject to a constitutional framework of legality, legitimate State purpose and proportionality. The Court's treatment of Section 57 reflected the concern that access by private entities to Aadhaar, without sufficient limitation on purpose, could lead to commercial use and profiling of individuals.

In the more interconnected land use matrix of Karnataka, these principles take on special importance. It is not that identity verification, database integration or digitisation per se is unconstitutional. Instead, the collection and use of this information should be connected to the legitimate purposes of registration, mutation or other State administered processes, and should be accompanied by protections commensurate with the informational risks involved. The concern is greater where identity data can be linked with ownership, transaction, financial or geospatial information from interconnected systems.

The constitutional framework thus supplements rather than replaces the provisions of the DPDP Act. The DPDP Act provides a statutory framework for the regulation of digital personal data, and Puttaswamy provides a general constitutional discipline for the regulation of State action that affects informational privacy. This is especially relevant in the land context as not all data-related issues are remedied by the DPDP Act per se, as set out above. Statutorily public land information may fall outside the scope of the Act under Section 3(c)(ii), and the correction rights under Section 12 do not necessarily apply to all types of land processing by the State. The core constitutional principles, such as legality and proportionality, are therefore also applicable to the design of digital land administration even if the exact remedy available under the statutory framework is restricted under the DPDP Act.

However, beyond the courtroom, field studies reveal significant exclusion caused by biometric failures, particularly among the elderly, manual laborers, and persons with disabilities—raising serious concerns about whether the scheme meets the principle of proportionality in practice.

8. Liability Beyond the State: Private Actors and Cybersecurity

The data structure of a property transaction goes beyond the State platform on which registration and land records are kept. Parties involved in financing an acquisition, collecting purchasing information, facilitating the transaction, searching for title and conducting due diligence, operating property-technology platforms, verifying identities, or providing cloud-based document and property-management services could capture or use parts of the same data set. The DPDP Act therefore introduces a private compliance layer to the digital land ecosystem, in addition to the obligations of the registration and revenue authorities.

An entity's industry classification doesn't dictate its legal character; its function does. Thus, if a bank decides what types of information are needed for a loan or KYC, a developer decides how information about users will be collected and used, or a platform used to purchase a property independently determines how such information will be processed, the persons making these decisions could be deemed to be Data Fiduciaries for the processing activities and operations that they carry out.[23] If a cloud-storage, CRM, verification or document-management service provider merely acts on behalf of that other entity, it could be a Data Processor. A single entity can be involved in multiple processing activities, playing different roles.

8.1 Accountability Across the Property-Data Chain

This distinction is relevant as it means that statutory accountability is not being outsourced when processing is outsourced. Once Rule 6 comes into force, it will require the Data Fiduciary to provide through its contract with the Data Processor for reasonable security safeguards, while Section 8(1) places responsibility on the Data Fiduciary for processing undertaken on its behalf by a Data Processor.[24]

This has a big impact on transactions involving property. The identity documents, financial

[23] Digital Personal Data Protection Act, 2023, § 2(i), (k), No. 22, Acts of Parliament, 2023 (India).
[24] *Id.* § 8(1); Digital Personal Data Protection Rules, 2025, r. 6(1)(f), G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India).

data, contact details, sale documentation or title material of the purchaser may pass through multiple technological layers without the responsibility of the entity that decides on the purpose and means of the processing of the information shifting. Vendor management is then no longer only a contractual or technical issue but a compliance one when it comes to data protection. Fragmentation of the technological chain does not, by itself, fragment the responsibility of the Data Fiduciary under the Act, in the case of a developer who relies on an external CRM, a lender who has a service provider that performs KYC services on its behalf, or a title-search platform that uses outsourced cloud infrastructure.

However, the DPDP framework would not make all the parties to a property transaction Data Processors of the other party(s). A broker, lender, developer or title-search provider who is in control of its own purpose and processing methods can be a Data Fiduciary, instead of simply a processor in another's chain. Why this functional classification is important — because the same documents are routinely being duplicated over and over again in various transactions involving properties. A compliance enquiry into a particular set of data should therefore include questions about who has the data, what is the purpose of their processing of it, who decides on that purpose and for whose benefit it is being processed.

The obligations become more significant when a party is notified as a Significant Data Fiduciary under Section 10. This could lead to higher obligations for large-scale processing of personal data where relevant entities or classes of entities are designated as Significant Data Fiduciaries, but such obligations should not apply without notification by the Central Government after considering statutory factors such as the volume and sensitivity of personal data processed and the risk to Data Principals. Once notified, a Significant Data Fiduciary is also subject to additional obligations under Rule 13, including due diligence in relation to technical measures such as algorithmic software.[25]

8.2 Retention, Erasure and Competing Legal Obligations

Private property actors also reveal an interesting qualification to the seeming conflict between permanent property records and the DPDP principle of erasure. Generally, a Data Fiduciary must delete personal data if consent is withdrawn or, earlier, as soon as it is reasonable to

[25] Digital Personal Data Protection Act, 2023, § 10(1), No. 22, Acts of Parliament, 2023 (India); Digital Personal Data Protection Rules, 2025, r. 13, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India).

believe that a specified purpose is no longer being pursued, and must ensure that the Data Processor with whom it has entered into a contract for processing erases the data provided for processing. The provisions also make an exception where retention is required for compliance with another law, as is done in Section 12 with respect to the Data Principal's right to erasure.[26]

That is not a general rule that data related to property is to be deleted when the transaction is finalized. Retention obligations may vary from participant to participant. For example, a lender has its own KYC/AML regime with its own needs for the preservation of customer-identification and transaction records. Statutory or regulatory retention does not replace the DPDP framework, but rather exists in addition to it.

The important difference is between retention because it is legally required, and retention on a purely ad hoc basis. There is no legal requirement for the retention of all ancillary datasets created as part of a transaction for the same length of time as a KYC record or a transaction document, or other specified material. It is important to consider additional types of copies such as copies made for internal coordination, copies of identity documents kept by intermediaries, CRM records, or unsuccessful enquiries/auxiliary profiling data which may need a new assessment of their continuing purpose and legal basis. The retention inquiry is therefore data- and purpose-specific, and not transaction-wide.

This distinction is reiterated in the final Rules. The deemed-purpose and erasure periods in Rule 8 are not a blanket deletion schedule for all Data Fiduciaries, but are specific to the classes of Data Fiduciaries and purposes listed in the Third Schedule.[27]The architecture is rather complex, however, in allowing for three different notions of erasure: not only purpose-based erasure but also minimum retention for specified regulatory purposes, and longer periods of retention mandated by other laws.

This means that for the property ecosystem, retention mapping is needed instead of uniform retention periods. Each participant should be able to distinguish between the legally required record and working copies and ancillary personal data, determine the legal basis for continued retention, and ensure the deletion of the corresponding record by the processors when the retention period has expired, or if the continuation of the retention is no longer justified. This

[26] Digital Personal Data Protection Act, 2023, §§ 8(7), 12(3), No. 22, Acts of Parliament, 2023 (India).
[27] Digital Personal Data Protection Rules, 2025, r. 8 & sched. III, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India).

is especially relevant when one piece of sale paperwork or an identity document has been spread amongst lenders, brokers, developers, document management systems and verification vendors.

8.3 Cybersecurity and Dual-Consequence Breaches

Information risk and property risk intersect most clearly in cybersecurity. Digital land transactions are associated with data sets that may hold identity data, ownership documents and records, sales documents, encumbrance documents, financial data and records for verification. Therefore, a compromise of these systems can have consequences other than the loss of confidentiality. In a land ecosystem where digital information is becoming more and more critical for verification purposes, integrity and availability are as important as protection against unauthorised disclosure.

Once operative, Rule 6 will require minimum reasonable security safeguards, such as encryption, obfuscation, masking or virtual tokens where appropriate; access controls; logging, monitoring and review; measures for continued processing after a personal-data breach; back-ups; contractual safeguards for processors; and technical and organisational measures securing compliance.[28] Rule 7 will also require a Data Fiduciary to notify each affected Data Principal of a personal-data breach without delay and requires an initial intimation to the Data Protection Board, followed by detailed information within seventy-two hours unless a longer period is allowed by the Board.[29]

These duties complement the broader framework of cybersecurity in India. In this regard, depending on the nature of the cyber incident, property-sector entities could be subject to potentially concurrent obligations with regard to cybersecurity and data protection, while also under an obligation to maintain logs of their ICT systems in accordance with CERT-In's directions for a period of 180 days.[30]

But the impact of a land breach should be judged not just on the grounds of the confidentiality of personal data. A disclosure of identity and transaction documents could lead to greater risk

[28] Digital Personal Data Protection Rules, 2025, r. 6, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India).
[29] *Id.* r. 7.
[30] Indian Computer Emergency Response Team, *Directions Under Sub-section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet*, No. 20(3)/2022-CERT-In, ¶ (iv) (Apr. 28, 2022).

of impersonation or misuse of documents; an integrity compromise could have adverse impacts on the integrity of data used for verification purposes; and loss of availability could cause loss of access to the documents and records used in registration, lending or mutation processes. The same incident then can create resulting informational harm under data protection law and transactional or proprietary consequences in property law.

The former is covered by the DPDP framework. Even if processing is outsourced to a processor, the Data Fiduciary is still obligated to adopt "reasonable security safeguards" and Rule 6 explicitly introduces the concept of processor security into the contractual framework. The Act does not, however, specify how the consequences of property loss resulting from a cyber incident are to be distributed amongst a registration authority, lender, developer, technology vendor, and/or other intermediary; nor does a DPDP proceeding alone rectify a changed land record or revive a stalled registration.

This creates an additional coordination problem. Data protection responsibility and property remediation are not the same. The first question is whether the personal information was processed lawfully and securely, and whether breach-related obligations were met; the second can be whether records are to be restored, whether the personal information is to be corrected in other interconnected systems of information, whether fraudulent use arising from the breach is to be prevented, or whether the legal consequences of a compromised transaction shall be resolved. A resilient digital land ecosystem therefore needs incident-response protocols: a link between cybersecurity remediation and the registration and revenue systems that protect the underlying property position.

The bigger picture is this: digitisation does not remove transactional risk, it simply shifts it. The property ecosystem in Karnataka is no longer restricted to the transferor and transferee and the registering authority as envisioned in traditional property law. Its reliance on a series of public databases and private technological intermediaries is growing, each potentially handling or moving the information that's needed for the transaction. The DPDP Act provides a valuable set of tools for allocating responsibility for personal-data processing, but it does not allocate every effect that could follow in the event of a simultaneous failure of the data layer and the proprietary layer. The latter requires sector-specific governance.

9. Toward a Privacy-Respecting Digital Land Registry

Karnataka need not have to choose between digitisation and informational privacy. Nor would

a return to records in hard copy create a better sense of security for titles. The objective should instead be to embed data protection into the very fabric of digital land administration. This is especially significant as Karnataka moves into the next phase beyond Kaveri 2.0: the State has announced the development of Kaveri 3.0, which has been described as a paperless, AI-based registration system, to be integrated with Asset Management Systems in all departments.[31] Deeper interoperability has already been achieved, so the move is an opportunity to consider privacy, accuracy and procedural measures at the design stage, as opposed to after the fact.

9.1 Separate Publicity of Title from Exposure of Personal Data

The fundamental rule should be to differentiate information which has to be available for the legal publicity of the title from information that on its merits is not necessary to disclose without restriction. The requirements of Section 57 of the Registration Act can't just be shelved to protect privacy - the reliability of access to registered transactions and encumbrances is required by purchasers, lenders and other interested parties. However, the process of digitisation does not have to be a perfect reflection of the original document's mode of access.

So, it is important for Karnataka to have a multi-layered access architecture. Basic information required for title work may be left publicly searchable, and any documents or fields with extra identity, contact and/or financial data may be protected by proportional measures such as authenticated access, masking, purpose-limited searches, or controlled certified copy mechanisms. Bulk extraction and automated scraping are not the same as a statutory inspection simply because both access a public record and should not be considered as such. This structure would enable the publicity function of registration but minimise the creation of easily aggregable personal profiles from individual property records.

9.2 Build Correction into Interoperability

Second, there is a need to accompany interoperability with an integrated correction mechanism. While Karnataka is connecting Kaveri with Bhoomi, e-Swathu and e-Khata and other departmental systems, incorrect data in one system can increasingly impact another system. The answer is not to make the citizen take the initiative in finding out which is the department that owns the failing datum and to initiate separate correction actions on each platform

[31] Government of Karnataka, Budget 2026–27, ¶ 432 (2026).

connected to it.

Each system objection should specify the source database, the data field in question and the data authority responsible for rectifying it. If the source record is updated, the correction should be transmitted to connected systems via an auditable update process, rather than continuing to rely on stale copies. The initial approach taken by Gilbert Vas, which saw the Karnataka High Court mandating a workflow between court decrees and Kaveri 2.0, Bhoomi and Mojini 2.0, is a clear example of how legal entitlements and digital workflows can be aligned through institutional and technical coordination.[32] The general approach being implemented problem-by-problem should be extended to become a general design principle: interoperability should transmit corrections as effectively as data.

9.3 Preserve Meaningful Human Review of Digital Objections

Third, more use of database verification does not make a technical mismatch a legal conclusion. The Registration Rules, 2025 already contain provisions relating to the reasons for not registering and appeal provisions. The next challenge is to make sure those protections are in place when the grounds for refusal are found in an integrated database, not in the Registering Officer's independent assessment.

An individual facing a digital objection should be informed of what went wrong, be able to challenge the information and be given human consideration when there is an error in the database which does not reflect the true legal position. This doesn't mean that automated verification must be given up. Automation is efficient at noticing inconsistencies—it should not make them practically impossible to review. Kaveri 3.0 needs to ensure that there is a dedicated exception pathway in cases where a party can establish that the system-generated result is in conflict with a court order, a corrected government record or other legally authoritative material.

9.4 Govern Data Flows, Not Merely Individual Databases

Fourth, interoperability should be the subject of governance in Karnataka. The State's Unified Land Management System is already linking multiple departments within a common

[32] Gilbert Vas v. State of Karnataka, W.P. No. 26357 of 2024, 2025:KHC:47151 (Karn. H.C. Nov. 14, 2025) (India).

architecture, and the process of land transactions and permissions is being increasingly coupled with e-Khata and Kaveri.[33] With these linkages growing and deepening, compliance can no longer be evaluated on a platform-by-platform basis.

The authority responsible for creating a new material data linkage must establish what information is being exchanged, what is the purpose for which that information is needed, where the information is derived from, the time period the information will be needed, and who will be given access and how errors will be corrected. This exercise may take the form of a data-protection and interoperability impact assessment for integrations that involve large amounts of personal data or affect individuals in significant ways. Such an assessment does not need to result in a parallel approval bureaucracy, but rather should make sure that technical integration is based on a defined legal and administrative goal and not simply the fact that data can be shared.

This should be applicable to private vendors as well. Agreements with cloud service, KYC service, CRM service and other processors should clearly outline allowed processing, security measures, data retention and data deletion obligations, notification of breaches, and data return or deletion in the event of the service relationship's termination. This would be the same fiduciary accountability model as provided by the DPDP Act, being applied to the structure of property administration.

9.5 Create a Land-Specific Incident and Accountability Protocol

Finally, response to cyber events must acknowledge that hacking into a land system can impact personal information, as well as proprietary interests. Breach notification alone will not cure a change in the ownership entry, nor will it resolve a registration blocked due to loss of access to an authoritative database.

Karnataka needs a coordinated incident protocol for digital land systems, so that there is a clear identification of the authorities to be contacted to manage the breach, maintain evidentiary logs, verify the integrity of records, flag potentially compromised transactions, and correct authoritative databases. If there is a private processor, the contract should allow for quick detection of the impacted data set and allocation of remediation responsibilities. The aim is not to view data-breach response and property-record remediation as two separate regulatory

[33] Government of Karnataka, Economic Survey of Karnataka 2025–26, ch. 12, § 12.1.22 (2026).

occurrences, but as one.

The establishment of a second land-registration system under the DPDP Act is not necessary for these reforms. They demand that the current system understand that the reliability of title is increasingly tied to the governance of the data on which the title is founded, recorded and accessed. Designing for privacy – in this context – involves more than reducing data gathering. It demands calibrated public access, traceable interoperability, effective correction, meaningful human review, accountable vendor relationships and cybersecurity measures that are powerful enough to safeguard informational and proprietary interests within the same digital record.

Conclusion

Karnataka stands at a turning point: land transactions are no longer only transfers of title—they are transfers of identity, metadata and personal information. The TPA ensures proprietary justice, whereas the DPDP Act ensures informational justice.

The DPDP Act read with its rules represents a significant milestone in India's privacy framework by introducing a mechanism for individuals to nominate a representative to manage their personal data after death or incapacity. This provision acknowledges the growing importance of digital footprints in modern life.

However, the DPDP Act stops short of creating a comprehensive legal architecture for digital legacy. Critical questions remain unanswered: Can digitized personal data be treated as an inheritable asset? Will future regulations integrate privacy rights with succession laws to enable structured devolution of digital assets? At present, the DPDP framework focuses only on privacy management, leaving broader issues—such as economic transfer, fiduciary responsibilities, and digital estate planning—outside its scope. As technology permeates every aspect of personal and financial identity, legislative and regulatory evolution in this domain is not just necessary but inevitable.

As Karnataka's land ecosystem becomes increasingly digital and interconnected, these two forms of justice can no longer operate in isolation. The challenge is not to choose between secure title and informational privacy, but to create land-governance systems that retain both forms of privacy. The next step in the digitisation process therefore needs to ensure both efficiency and interoperability, along with accurate records, proportionate access, meaningful

review and data security. In a digital land ecosystem, protecting the integrity of title goes hand in hand with protecting the integrity of the data through which title is established, verified and transferred.