Digital Twin Data Regulation: Balancing Urban Innovation and Cyber Risk In India

Poorna K[1], Harinibai. R[2]
[1,2]*Sastra Deemed to be University*

Abstract—**Digital twin technology (DTT) has emerged as a keystone of smart city innovation, enabling real-time digital replicas of physical infrastructure for development, monitoring and predictive analysis. By integrating sensors, cloud computing, artificial intelligence (AI) and Internet of things (IoT) devices, digital twins enhance efficiency and urban decision making. However, this interconnected ecosystem also heightens vulnerability to cyber threats such as data manipulation, hacking and corruption of AI models that can disrupt infrastructure, compromise operational data and jeopardize public safety. India's existing legal framework remains ill- equipped to govern these risks. The Information technology Act,2000 primarily addresses e- commerce and e-governance, while the Digital personal data protection (DPDP) Act,2023 safeguards only personal data, leaving sensor-based, non-personal and machine generated datasets unregulated. The proposed Digital India Act outlines broad digital principles with no specific mechanisms for non-personal or machine generated data. The National Data Governance Framework Policy (NDGFP, 2022) is a non-binding policy draft, limited to government-held datasets, Although the Kris- Gopalakrishnan Committee Report (2020) proposed foundational principles for non-personal data governance, it remains unimplemented and silent on liability, standards and institutional safeguards. In contrast the European Union's Data Act, 2023 establishes a comprehensive framework for both personal and non-personal data sharing, interoperability and protection. This paper argues that India requires a dedicated non-personal data governance law that operationalises the Kris committee's recommendations, integrates cybersecurity and accountability provisions and safeguards the data infrastructure underpinning national initiatives such as the SANGAM Digital Twin.**

Index Terms—**Digital Twin Technology, Cybersecurity, Non-Personal Data, Internet of things (IOT).**

I. INTRODUCTION

Technological developments in recent times have delivered advances in terms of wireless and mobile communications, ever-present connectivity, improved communication speeds and cheaper sensors. Not only has technology become increasingly pervasive but there has also been closer integration between cyber systems and physical infrastructure, more commonly referred to as the Internet of Things (IoT). Falling costs and advances in communication networks have resulted in the rapid uptake of this technology in recent years. Consequently, this presents numerous opportunities for knowledge of the built environment to yield considerable value.[2]

Digital Twin Technology (DTT) represents a ground-breaking innovation that bridges the physical and digital worlds. A digital twin is a virtual model of a physical object, process or system that mirrors real-world conditions in real time through continuous data exchange using sensors, Artificial Intelligence (AI), cloud computing and the Internet of Things (IoT). This dynamic representation allows simulation, monitoring and predictive analysis, enabling smarter and more efficient decision-making across industries. There is growing recognition of the opportunities presented by digital twins and the IoT in the built environment. From 2022 to 2030, the digital twin model is actually expected to develop at a 39.48% CAGR.[3] This contributes to the creation of smart cities to facilitate information sharing with the public. However, while they offer numerous benefits, there are also a number of associated challenges and chief among these is the security threat. At present, there are distinct challenges when attempting to install cybersecurity into digital twins that will be utilised in applications designed for the built environment.

II. RESEARCH METHODOLOGY

This study uses a doctrinal research method to analyse the statutes, policy documents and expert reports. It examines primary and secondary sources, including the Information Technology Act, 2000, the Proposed Digital India Act, 2023, National data governance policy framework, 2022 and the Kris Gopalakrishnan Committee Report (2020).

A comparative approach is also adopted, focusing on the European Union Data Act (2023) to identify global best practices for regulating non-personal and machine-generated data. Secondary sources such as government press releases and official portals on the Sangam Digital Twin initiative supplements the analysis. Through this doctrinal analysis, the paper aims to propose a dedicated Non-Personal Data Governance Law to strengthen cybersecurity and data governance for digital twin ecosystems in Indian smart cities.

Digital Twin Technology in India

Digital Twin Technology (DTT) represents one of the most transformative innovations which creates a virtual replica of physical assets, systems or environments that mirrors real-time conditions through continuous data inputs from sensors and Internet of Things (IOT) devices. These replicas enable advanced monitoring, simulation and predictive analytics, allowing policymakers and engineers to make informed, data-driven decisions about designs, maintenance and resource management. By integrating Artificial Intelligence (AI), machine learning (ML) and cloud computing, digital twins facilitate optimization across multiple sectors including transportation, energy, construction and healthcare thereby reducing operational costs while improving efficiency and sustainability. In short, a digital twin functions as a living, data-driven mirrors of the physical world that evolves continuously alongside it.[4]

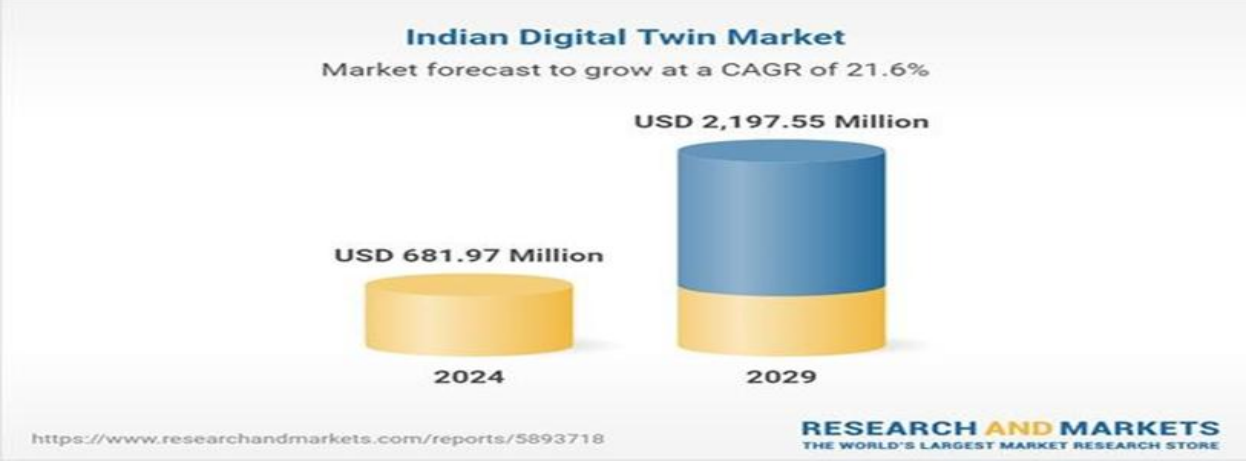

Figure 1: Market forecast of digital twin in India[5]

Globally, governments and industries are increasingly adopting DTT to modernize infrastructure and promote urban resilience. The Government of India through its "Digtial India" vision has recognized DTT as a crucial enabler for next generation public infrastructure planning. The most prominent example is the "SANGAM: Digital Twin" initiative, launched by the Department of Telecommunications (DoT) under the ministry of Communications.[6] The initiative symbolizes a collaborative national effort to develop a unified digital ecosystem that leverages real-time data and geospatial analytics for infrastructure planning, monitoring and decision-making.[7]

The Sangam Digital Twin Project aims to build Proofs of Concept (PoCs) that integrate multiple data sources, satellite imagery, sensors and urban planning models to create dynamic digital replicas of India's infrastructure networks.[8] It envisions a framework where various stakeholders, central and state governments, private companies and research institutions collaborate to use these virtual environments for predictive analysis and sustainable

city management.[9] According to the project's official portal, Sangam seeks to "build a Digital Twin ecosystem that facilitates responsive planning, efficient design and real-time governance using live data streams."[10] The initiative also underscores the role of DTT in reducing infrastructure costs, improving commuter experiences and enabling data-driven insights for long-term sustainability.[11]

Moreover, Sangam aligns with India's larger goal of becoming a $1 trillion digital economy by 2026, positioning digital infrastructure as a driver of inclusive growth. It embodies a convergence of technologies such as IoT, AI, 5G and geospatial intelligence, reflecting the government's commitment to evidence-based policymaking and digital governance.[12] However, while the potential benefits of digital twins are immense, their implementation introduces significant legal and regulatory challenges, particularly regarding the protection, governance and ethical use of non-personal data (NPD). As DTT systems depend on massive sensor-based datasets that record real-time activity in public and private spaces, issues of data ownership, cybersecurity and accountability become critical. Yet, India currently lacks a dedicated legal framework to govern non-personal, machine-generated data, creating a major policy vacuum that this paper seeks to address.

Concept of Digital Twin Technology

Digital Twin Technology (DTT) refers to the creation of a virtual, real-time digital replica of a physical asset, system or environment, generated through continuous data inputs from Internet of Things (IoT) sensors, communication networks and cloud-based analytical platforms. A digital twin mirrors the current state of its physical counterpart and enables simulation, predictive modelling and remote monitoring. In smart infrastructure ecosystems, DTT integrates terminal-layer IoT devices, fog-layer processing nodes and cloud-layer data centers, forming a vertically layered architecture that supports continuous data acquisition and intelligent decision-making.[13] Through this multilayer structure, raw sensor data are collected, pre-processed at the edge to reduce latency and then transmitted to cloud servers for complex analytics, predictive maintenance and long-term infrastructure planning.

The expansion of smart cities globally has accelerated the adoption of digital twin systems. Smart cities rely intensively on sensor-rich IoT networks embedded in traffic systems, environmental monitors, public utilities, smart grids, surveillance systems and mobility infrastructure. The smart-city architecture described in the literature demonstrates that IoT devices interact with gateways and fog nodes to support real-time applications requiring low latency and large-scale data analysis.[14] Digital twins function as the digital layer of this ecosystem, enabling city administrators to observe real-time conditions, simulate hypothetical scenarios, anticipate disruptions and optimize resource allocation.

However, the same interconnectedness that makes DTT powerful also renders it highly vulnerable to cyber-attacks. IoT-based smart city systems suffer from a dramatically expanded attack surface due to billions of heterogeneous devices, limited device-level security and reliance on wireless communication. These devices often lack strong cryptographic capabilities

because of resource constraints, making them easy targets for attackers.[15] The literature identifies a wide range of cyber threats, all of which can penetrate IoT infrastructure and compromise the digital twin layer built on top of it.[16] Smart-city IoT components are typically deployed in unattended or publicly accessible environments, enabling attackers to physically tamper with, replace or infect devices. Once compromised, malicious actors can inject manipulated sensor data, corrupt communication between fog and cloud layers or poison machine-learning models that underpin predictive analytics. As a result, a digital twin, whose core function is to reflect real-time truth, may begin operating on false data, leading to faulty simulations and dangerous administrative decisions. Moreover, research shows a dramatic global increase in IoT-related cyber incidents, with Symantec reporting nearly a 600% rise in IoT attacks in recent years.[17] Such statistics illustrate the scale of risk facing digital twin ecosystems.

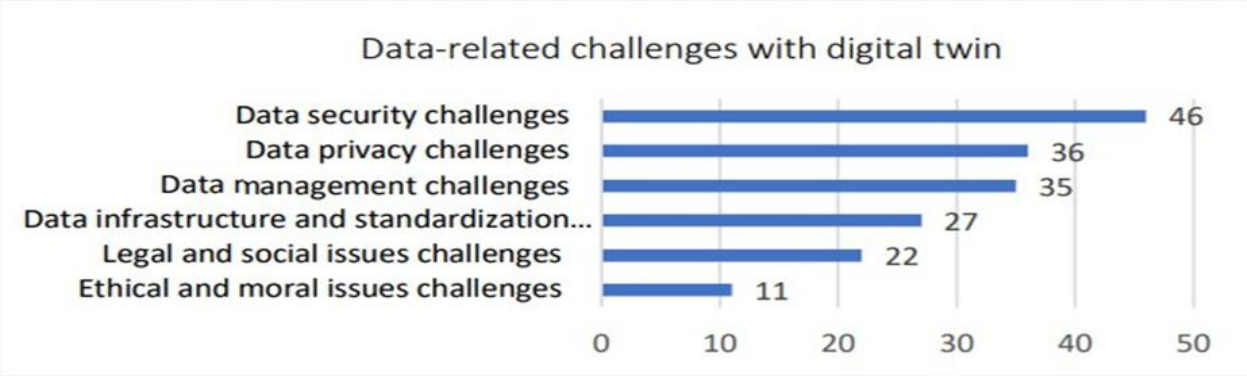

Figure 2: Data related challenges with Digital Twin[18]

These vulnerabilities underscore the urgent need for legal and regulatory frameworks governing non-personal, machine-generated data. The data flowing into digital twins are predominantly non-personal datasets, including environmental readings, traffic patterns, structural integrity metrics and utility consumption indicators. While these datasets do not identify individuals, they are nonetheless essential to national infrastructure stability. Yet, India currently lacks statutory rules defining ownership of such data, enforcing cybersecurity standards, imposing accountability for data corruption or regulating cross-sectoral and cross- border data sharing.

Therefore, as India advances digital initiatives such as the Sangam Digital Twin ecosystem, there is a compelling need to regulate non-personal data to ensure data integrity, cybersecurity, accountability and national resilience.

Existing and Proposed Legal Framework in India

1. Limitations of the Information Technology Act, 2000 in Governing Digital Twin Data and Non-Personal Machine-Generated Data

The Information Technology Act, 2000 (IT Act) is structurally inadequate for governing Digital Twin ecosystems because it was enacted to regulate electronic records, e-commerce authentication and computer crimes, not complex, real-time, cyber-physical infrastructure systems that rely on machine-generated non-personal data. Its scope is narrow and its substantive provisions do not address operational cybersecurity, liability allocation or data- integrity standards needed for IoT-driven Digital Twin environments.

First, the IT Act contains no statutory definition of non-personal data, machine-generated data or IoT sensor data; which means Digital Twin datasets fall outside any meaningful data- governance framework. Second, the Act does not create sector-specific cybersecurity standards: Section 43 penalises unauthorised access and damage to computer resources, but does not mandate encryption, secure API design, penetration testing, audit trails or operational resilience standards for critical infrastructure which are the elements essential for protecting Digital Twin models from data manipulation, sensor spoofing. Third, Section 43A, the only provision addressing data security practices, applies only to "body corporates handling sensitive personal data," meaning it expressly excludes non-personal and machine-generated operational data, which forms the backbone of Digital Twins. The Act therefore provides no liability when a cyber-attack compromises real-time infrastructure data, disrupts public utilities or corrupts AI models controlling Digital Twin systems. Fourth, Section 66 defines computer- related offences but focuses on intentional unauthorised acts; it does not cover negligent cybersecurity lapses, insecure IoT deployments, poor encryption, default passwords or supply- chain vulnerabilities are the major causes of Digital Twin ecosystem breaches. Also, the Act lacks provisions on data integrity, or real-time authenticity, which are crucial when Digital Twin systems rely on continuous sensor feeds that can be tampered with. The IT Act has no mechanism for assigning liability in multi-stakeholder ecosystems: smart city Digital Twins involve device manufacturers, network providers, cloud hosts, analytics vendors and municipal authorities, yet the Act contains no rules for shared responsibility, no vicarious liability clauses

and no joint-controller framework for machine-generated datasets. The Act is technologically outdated, it predates IoT, AI, cloud computing and Digital Twin architectures and therefore cannot be interpreted expansively without violating the principle of legality (courts cannot stretch a penal statute beyond its clear language). It does not address issues related to AI-driven decision-making, the operation of interconnected IoT devices that continuously feed data into digital twin models.[19]

Thus, the IT Act remains inadequate, outdated and insufficient for securing Digital Twin ecosystems, protecting non-personal machine data or ensuring liability for breaches that affect real-world infrastructure, thereby necessitating both short-term amendments and a future dedicated statute for machine-generated non-personal data governance.

2.Digital Personal Data Protection Act, 2023 (DPDP Act)

The DPDP Act, 2023, represents India's first dedicated law on personal data protection, and was enacted in line with GDPR in the EU, to safeguard individual privacy in the digital age. It ensures a comprehensive and coherent approach to the free movement of all data in the EU and provides more clarity to businesses on how to handle data across borders the Commission has published informative guidance.

a. Scope and Applicability

The Preamble of the DPDP Act, 2023, states, "An Act to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto." It applies exclusively to data about a person identifiable in relation to such data. Therefore, datasets produced by sensors, industrial systems, or urban infrastructure, such as environmental readings, building energy metrics, or AI simulation outputs are outside its scope.

b. Impact on Digital Twin Systems

Digital twins depend on large-scale, real-time, non-personal datasets generated by IoT devices and municipal infrastructure. Since this data does not identify individuals, it is unregulated under the DPDP Act. Consequently, the collection, processing, and sharing of such data remain legally unmonitored, creating risks of misuse, manipulation, or cyber exploitation.

c. Limitations

While the DPDP Act introduces progressive principles like data minimization, purpose limitation, and data fiduciary accountability, these apply only to personal data ecosystems. The exclusion of non-personal data leaves no statutory protection or liability framework for entities handling critical smart city datasets. This omission weakens India's preparedness for cybersecurity governance in digital twin applications.

In essence, the DPDP Act's narrow focus results in fragmented data protection, where personal data is safeguarded, but machine-generated operational data which does not pertain to a particular person but has a real-world impact, and which is equally vital for national security and governance infrastructure remains outside the law.

3.Limitations of NDGFP with respect to digital twin ecosystems:

The National Data Governance Framework Policy (NDGFP), represents an important conceptual step in India's non-personal data governance landscape; however, it remains structurally insufficient for the regulation of Digital Twin ecosystems that depend on high- frequency, machine-generated operational data sourced from IoT sensors. As a policy rather than legislation, the NDGFP is non-binding, framed in permissive terms such as "encourage," "may contribute," and "should adopt," which, under the literal rule of interpretation, cannot impose enforceable legal obligations on government ministries or private entities involved in Digital Twin deployments.[20] This non-binding character poses immediate challenges for public–private Digital Twin systems such as the SANGAM initiative, where significant portions of operational telemetry are generated and controlled by private vendors; without statutory mandate or explicit contractual assignment, such private actors cannot be compelled to share real-time IoT data essential for critical infrastructure modelling.[21] Further, the NDGFP fails to define or recognise machine-generated data or real-time operational datasets, instead treating all non-personal data homogeneously. The principle of expressio unius est exclusio alterius suggests that the omission of these critical data categories reflects an intention not to govern them within this framework.[22]

Although the NDGFP allows the Government to classify datasets as "high-risk", including those concerning national security, nuclear facilities and critical infrastructure,[23] it simultaneously excludes such datasets from sharing without providing a parallel mechanism for their cybersecurity, data integrity or operational protection. This omission is particularly consequential for Digital Twin systems used in mobility management, energy distribution, water networks and emergency response, domains where the corruption, manipulation or delay of data can translate into direct physical-world harm. The NDGFP White Paper explicitly states that it "does not address data security issues," leaving Digital Twin infrastructures entirely outside any mandatory cybersecurity framework for encryption, secure APIs, authentication protocols, penetration testing or coordinated vulnerability disclosures.[24] In addition, the policy provides no liability regime, penalties or adjudicatory structures in cases where unauthorized access, negligent handling or data manipulation of Digital Twin datasets results in operational disruption. This violates the purposive interpretation principle, which requires that legal instruments intended to facilitate safe and fair data use must also create accountability structures. The NDGFP further suffers from ambiguity regarding private-sector data holders, merely "encouraging" them to contribute datasets without establishing compulsory mechanisms, valuation frameworks or FRAND-like principles for essential IoT feeds. This undermines interoperability and creates fragmented Digital Twin deployments across states and municipalities.

Additionally, the NDGFP is silent on cross-border transfers of non-personal critical infrastructure data, posing data-sovereignty risks where Digital Twin platforms rely on foreign cloud providers or offshore processing. Unlike the EU Data Act, which articulates strict rules for cloud portability, switching and foreign government access,[25] the NDGFP provides no such safeguards. The policy also lacks detailed anonymization standards such as re-identification thresholds, differential privacy parameters or independent audits, rendering it inadequate for highly granular Digital Twin datasets that can easily be re-identified when correlated with auxiliary information.[26] Collectively, these limitations demonstrate that the NDGFP does not meaningfully govern or secure Digital Twin ecosystems, leaving a regulatory vacuum that requires, a dedicated Non-Personal and Machine-Generated Data Governance Law tailored to the cyber-physical sensitivities of Digital Twin technologies.

3.Proposed Digital India Act, 2023 and its limitations:

The proposed Digital India Act (DIA), although envisioned as a successor to the two-decade- old IT Act, remains fundamentally inadequate for governing non-personal data (NPD) and machine-generated data that power Digital Twin ecosystems and smart-city infrastructures. First, the DIA consultation documents and Ministerial briefings explicitly state that the Act will primarily focus on user safety, platform regulation, intermediary obligations, cybercrime, digital competition and emerging technologies, but do not propose any substantive framework for NPD governance. The policy emphasis remains anchored around personal data protection, online harms and intermediary accountability, leaving a complete regulatory vacuum for industrial IoT data, real-time operational telemetry, AI model training datasets and Digital Twin sensor streams, which constitute the majority of infrastructural data in smart cities. Applying the literal rule, the DIA's draft objectives and scoping language do not mention NPD, sovereignty over machine-generated data, shared access obligations or standards for secure processing of operational datasets. Under the principle of expressio unius est exclusio alterius, this silence indicates a deliberate exclusion: by expressly emphasising personal data and online platforms and omitting non-personal datasets, the legislature cannot be assumed to govern them indirectly. Second, the DIA retains the intermediary-liability model of the IT Act, which is inherently incompatible with Digital Twin systems, because the actors managing machine- generated data (OEM manufacturers, sensor integrators, cloud hosts, analytics firms, system operators) are not "intermediaries" within the statutory sense. Therefore, they escape obligations entirely. Third, the DIA proposes no data-sharing mandates, access rights, usage rights or rights over machine-generated data, unlike the EU Data Act, which explicitly distinguishes personal and non-personal industrial data and grants rights to users, manufacturers and public bodies. Without such provisions, government bodies cannot access IoT data necessary for national infrastructure monitoring, nor can smart-city operators claim rights

over data generated by private vendors creating legal uncertainty in PPP-based Digital Twin projects such as the Sangam initiative. Fourth, the DIA includes no cybersecurity obligations specific to NPD or machine-generated telemetry. It continues the generic offence-based approach of the IT Act without creating mandatory security standards for IoT devices, AI models, encryption of sensor feeds, integrity of real-time data flows or resilience of cyber- physical systems. The omission is significant because Digital Twin attacks do not always
constitute "cybercrimes" but often involve data poisoning, sensor spoofing, model corruption or operational interference, none of which are categorised under the DIA's proposed cyber- offence framework. The mischief rule reinforces that the DIA's purpose is not to regulate cyber-physical operational risks, but to modernize online safety and platform accountability; hence, interpreting it to include Digital Twin data governance would exceed its legislative intent.

Finally, the DIA does not propose a national structure comparable to the Data Governance Authority suggested by the Kris Gopalakrishnan Committee, nor any mechanism for anonymisation standards, NPD valuation, competition safeguards, data portability or FRAND- based access to industrial datasets. The absence of these pillars renders the DIA structurally incapable of regulating Digital Twin ecosystems. Consequently, even after the DIA is enacted, India will continue to lack a dedicated legal framework for non-personal data and machine- generated data, necessitating a separate NPD law or an amendment addressing this domain explicitly.[27]

Comparative Analysis: The EU Data Act and the NDGFP, Identifying Gaps and Necessary Reforms for India's Non-Personal Data Governance

India's National Data Governance Framework Policy (NDGFP), 2022, represents the country's first structured attempt to create an ecosystem for sharing anonymised non-personal data (NPD). However, it remains a policy instrument without statutory backing, limited primarily to government-held datasets and lacking enforceable obligations for private entities. In contrast, the European Union's Data Act establishes one of the world's most comprehensive legal frameworks governing both personal and non-personal data generated by connected devices, industrial systems and IoT networks. A comparison between the two reveals significant gaps in the NDGFP and highlights the reforms required for India to build a robust governance regime suited to emerging technologies such as Digital Twin systems.

1. Access Rights over Data Generated by Connected Devices

The EU Data Act creates a legally enforceable right for users of connected devices to access all data generated by their use of such devices in a "structured, commonly used and machine- readable format." Manufacturers and service providers must ensure secure, immediate and direct access mechanisms and cannot unreasonably withhold or delay access. This includes a right to share such datasets with third parties of the user's choice.[28]

By contrast, the NDGFP only envisions access to government-held non-personal data through the India Datasets Program, with no provision granting users (citizens, enterprises or organisations) the right to access or utilise machine-generated data from private IoT systems, smart infrastructure or industrial operations. To align with international standards, the NDGFP must recognise user access rights over NPD generated by devices they operate or own, especially where such data feeds into critical systems such as Digital Twin infrastructures.

2. Fair, Reasonable and Non-Discriminatory (FRAND) Data-Sharing Obligations

Under the EU regime, data-sharing contracts must be fair, reasonable and non-discriminatory. Data holders may charge compensation, but abusive or one-sided contractual terms are prohibited and SMEs receive additional protections. This creates a balanced environment for innovation while preventing monopolisation of industrial data by large corporations.[29]

The NDGFP, lacking legislative authority, does not impose any binding obligations on private entities to share NPD equitably or prevent discriminatory pricing. Incorporating FRAND-based obligations would help India develop a level playing field, particularly essential for startups, research institutions and small enterprises that rely on access to non-personal datasets for innovation in the Digital Twin ecosystem.

3. Public-Sector Access to Private-Held NPD During

Emergencies

A key provision of the EU Data Act is Business-to-Government (B2G) data access in "exceptional circumstances," such as natural disasters, public health emergencies or infrastructure failures. Public authorities may request specific non-personal data from private entities, subject to strict safeguards, proportionality and compensation mechanisms.[30]

The NDGFP contains no equivalent provision for accessing private-sector NPD, even in emergencies. This gap is critical for urban digital infrastructure, where real-time sensor data from private operators (e.g., mobility apps, energy providers, telecom IoT systems) may be

vital for smart-city management. India must introduce a B2G access mechanism with clear legal safeguards, transparency requirements and narrowly defined emergency triggers.

4. Interoperability, Portability and Cloud Switching

The EU Data Act mandates interoperability standards, common data schemes and the removal of contractual and technical barriers to switching cloud providers.[31] This prevents vendor lock- in and ensures that industrial and infrastructural data remain portable across platforms. NDGFP addresses metadata standards for government datasets but does not create a nationwide interoperability architecture or regulate cloud-service portability. For Digital Twin systems, where multiple agencies, vendors and platforms exchange real-time machine-generated data, interoperability is essential. India must therefore incorporate statutory requirements for open standards, API-based interoperability and multi-vendor portability.

5. Trade-Secret Protection and Contractual Fairness

The EU Data Act strikes a balance by requiring data sharing while protecting trade secrets. It prohibits forced disclosure of proprietary algorithms or commercially sensitive inferences and it introduces dispute resolution mechanisms for unfair contractual terms.[32]

NDGFP offers only high-level guidance and lacks a concrete legal shield for proprietary technologies. This discourages private companies from contributing to national datasets. India should introduce trade-secret protection clauses, contract-fairness rules and standard-form agreements to build trust between government and private sector data contributors.

6. Cross-Border Transfer Safeguards

The EU Data Act includes explicit safeguards against unlawful non-EU governmental access, requiring encryption, audits and transparency reports for cross-border NPD transfers.[33]

The NDGFP does not address cross-border NPD at all. As digital twin systems increasingly rely on foreign cloud storage and global data infrastructure, India needs a rigorous framework specifying: conditions for cross-border transfer of NPD, restrictions for critical infrastructure data, compliance requirements for foreign cloud providers and mechanisms to prevent unlawful foreign surveillance.

7. Enforcement and Accountability

The EU Data Act has the force of law, backed by supervisory authorities with investigative and enforcement powers.[34] NDGFP is purely policy-based, lacking penalties, obligations or oversight mechanisms.

Limitations of the Kris Gopalakrishnan Committee Report and the Need for a Dedicated NPD Law

The Kris Gopalakrishnan Committee Report (2020) was India's first comprehensive attempt to articulate a framework for the governance of non-personal data (NPD), but despite its conceptual clarity, the Report remains structurally inadequate to regulate the complex, real- time, machine-generated data ecosystems that underpin emerging technologies such as Digital Twin systems in smart cities. The Report's primary focus is on enabling data sharing for economic value creation and innovation, setting out definitions for non-personal data, sensitive NPD, community data and the roles of data trustees and data custodians. [35] However, it does not impose any statutory obligations concerning how NPD must be collected, processed, secured or shared, nor does it provide any enforceable rights to stakeholders. It explicitly proposes only a conceptual governance architecture, leaving the actual legal mechanisms, rights, duties, standards, penalties, enforcement structures are unaddressed.[36] As a result, the Report functions more as a recommendatory policy document than a regulatory instrument capable of safeguarding critical NPD in cyber-physical infrastructure.

Moreover, the Committee's framework does not articulate cybersecurity standards for non-personal data, notwithstanding the fact that NPD generated by sensors, IoT devices, industrial systems and urban digital infrastructure is susceptible to tampering, manipulation and cyberattacks. The Report offers no provisions on data integrity verification, breach reporting, authentication mechanisms or liability in the event of data corruption or misuse. These omissions are significant, particularly given that Digital Twin systems rely entirely on continuous, high-trust, machine-generated NPD for simulations, predictions and operational decision-making.

A further limitation is the absence of a legally recognisable mechanism for Business-to- Government (B2G) access to privately held NPD. The Committee highlights the importance of

community data and the need for sharing datasets for public interest purposes,[37] yet it does not provide a binding framework to compel private entities to share relevant NPD with public authorities, even when such data is essential for governance, emergency response or infrastructure management. This makes the framework impractical for real-world implementation where private actors control large volumes of urban sensor data. Another major weakness of the Report is its ambiguous treatment of community data. While it introduces the notion of data derived from a group of people and vests responsibility in "data trustees," it does not clarify fundamental questions: who legally owns community data, how consent is to be obtained collectively, how rights are to be exercised, how conflicts are resolved or how benefits from such data are to be shared. This creates uncertainty and potential disputes, undermining the possibility of using community-derived NPD for civic applications, including Digital Twin governance.

Additionally, the Committee does not address the increasingly critical issue of cross-border transfer of non-personal data. Given that much of India's machine-generated infrastructural data is stored on foreign cloud servers, the absence of rules on localisation, conditions for cross- border transfer or safeguards against foreign government access constitutes a serious regulatory vacuum. Further, although the Report proposes a Non-Personal Data Authority (NPDA), this body lacks statutory backing, defined powers or enforcement mechanisms.[38] Without legislative force, the NPDA cannot mandate compliance, conduct audits, impose penalties, ensure cybersecurity or resolve disputes. Consequently, the Committee's recommendations, though conceptually insightful, fall short of creating an actionable, enforceable governance regime.

Taken together, these structural deficiencies demonstrate that the Kris Gopalakrishnan Committee Report cannot serve as the foundation for India's NPD governance framework. The absence of statutory obligations, accountability provisions, cybersecurity mandates, cross- border safeguards and enforceable rights render the framework inadequate for a data-driven, sensor-dependent, Digital Twin-enabled governance environment. India therefore requires a dedicated Non-Personal Data Governance Act or a comprehensive NPD chapter within the

forthcoming Digital India Act, to establish binding standards and protections aligned with global best practices.

Digital twin strategy for India

The Digital Twin Strategy for Indian Infrastructure report outlines an ambitious national vision to deploy Digital Twin technologies across roads, highways, railways, energy systems and urban infrastructure, emphasising the need for continuous, high-quality, machine-generated data to support real-time monitoring, predictive analytics and infrastructure optimisation.[39] While the Report recognises the transformative potential of Digital Twins and calls for integrated data platforms, interoperability across systems and advanced digital capabilities, it does not propose a corresponding legal or regulatory structure for the governance, security or accountability of non-personal datasets that would feed these systems. When read alongside the Kris Gopalakrishnan Committee Report which offers conceptual frameworks for non-personal data but lacks enforceable obligations or cybersecurity safeguards it becomes evident that India is moving ahead with Digital Twin deployment without a legally robust data governance foundation. This growing disconnect between technological ambition and regulatory preparedness reinforces the need for a dedicated Non-Personal Data Governance

Act that can establish binding standards, define rights and duties, regulate private-sector data access and ensure the integrity and security of machine-generated data essential to Digital Twin ecosystems.

III. CONCLUSION

Digital Twin Technology (DTT) marks a major shift in India's transition toward data-driven and cyber-physical governance, especially in smart cities and national infrastructure sectors. Government initiatives such as SANGAM: Digital Twin and the Digital Twin Strategy for Indian Infrastructure demonstrate that India is actively building the technological foundation for real-time modelling, predictive analytics and integrated digital infrastructure management. However, this rapid technological adoption stands in contrast to the fragmented and incomplete legal landscape governing the underlying non-personal data (NPD). The Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 and the National Data Governance Framework Policy (NDGFP) collectively address only cyber offences, personal

data and government-held datasets, leaving machine-generated, sensor-based and infrastructural NPD largely outside any statutory protection. The Kris Gopalakrishnan Committee Report, though pioneering in introducing conceptual categories for NPD, remains non-binding and lacks enforceable rights, cybersecurity obligations, liability mechanisms and cross-border safeguards. This creates a significant regulatory vacuum in precisely the domain where NPD forms the lifeblood of Digital Twin ecosystems. Without a robust statutory framework, India faces risks relating to cyber manipulation, operational failures in smart-city infrastructure, monopolisation of essential datasets by private actors and unchecked cross- border transfers of critical infrastructural data. Therefore, the evidence clearly demonstrates that India's technological ambitions have surpassed its regulatory preparedness, necessitating a unified, statutory and future-ready mechanism to govern NPD in a manner consistent with global best practices.

IV. SUGGESTIONS

India requires a distinct statutory instrument that complements the DPDP Act but is specifically tailored to regulate the collection, processing, sharing and protection of non-personal and machine-generated data. Such a framework must not only address ownership and access but also establish accountability for algorithmic decision-making, cross-border data transfers and cybersecurity compliance within complex digital ecosystems like DTT. Such a framework should:

4.1 Introduce mandatory cybersecurity and data-integrity standards for all machine-generated datasets used in critical infrastructure, including encryption, authentication, logging and tamper-detection protocols.

4.2 Establish clear, enforceable liability and penalty mechanisms for data corruption, unauthorised access, system manipulation and breaches affecting non-personal datasets.

4.3 Harmonise India's regulatory framework with global best practices, including interoperability mandates, access rights and FRAND-based data-sharing norms under the EU Data Act.

4.4 Create a sector-specific, role-based liability structure ensuring that each stakeholder in the DTT ecosystem device operators, algorithm developers, cloud platforms, data custodians bear proportionate responsibility for risks arising from their technical and operational roles.

By adopting these reforms, India can ensure that the rapid integration of Digital Twin Technology into smart-city governance is supported by robust legal safeguards. A well- designed NPD framework will not only strengthen technological reliability and urban resilience but also secure public safety and national security as India transitions into a data-driven, cyber-physical governance era.

REFERENCES

Statutes & Policies

[1] The Information Technology Act, 2000, No. 21 of 2000, India Code.

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

[3] National Data Governance Framework Policy, Ministry of Electronics & Information Technology (2022).

[4] Regulation (EU) 2023/2854 of the European Parliament and of the Council, Data Act, Dec. 13, 2023, 2023 O.J. (L 2023/2854).
[5] Kris Gopalakrishnan Committee Report on Non-Personal Data Governance Framework (2020), Ministry of Electronics & Information Technology.

Government Websites, Sangam Digital Twin Initiative

[1] SANGAM: Digital Twin Initiative, Department of Telecommunications, Telecommunication Centres of Excellence (TCoE) India, https://sangam.tcoe.in/about
[2] About EoI: Digital Twin – Sangam, Telecommunication Centres of Excellence (TCoE) India, https://sangam.tcoe.in/about-eoi
[3] Press Release, Press Information Bureau, Sangam: Digital Twin Initiative of the Department of Telecommunications (Apr.1,2024), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2032825

Academic Articles

[1] Kaznah Alshammari, Thomas Beach & Yacine Rezgui, Cybersecurity for Digital Twins in the Built Environment: Current Research and Future Directions, 26 J. Info. Tech. in Constr. 159 (2021).
[2] Marija Kuštelega, Renata Mekovec & Ahmed Shareef, Privacy and Security Challenges of the Digital Twin: Systematic Literature Review, 30 J. Universal Computer Sci. 1782 (2024).
[3] Digital Twins: Real-Time Monitoring Transforming India's Infrastructure Lifecycle, EPC World (Oct. 2024), https://www.epcworld.in/digital-twins-real-time-monitoring- transforming-indias-infrastructure-lifecycle
[4] Jeffy Jacob, Nitin Gadkari Unveils Digital Twin Strategy for Infrastructure, Geospatial World (Mar. 2024), https://geospatialworld.net/prime/business-and-industry-trends/nitin-gadkari-unveils-digital-twin-strategy-infrastructu
[5] reLabanya Prakash Jena, Digital Twin: Making India's Clean Energy Architecture Versatile, Observer Research Foundation (Jan. 2024), https://www.orfonline.org/expert-speak/digital-twin-making-india-s-clean-energy- architecture-versatile
[6] India Digital Twin Market, Competition, Forecast & Opportunities, 2029, Research and Markets (2023), https://www.researchandmarkets.com/report/india-digital-twin- market
[7] Tata Consultancy Services, Proposed Digital India Act 2023 — Digital India Dialogues (Mar. 9, 2023), https://www.tcs.com/content/dam/tcs/pdf/discover- tcs/investor-relations/faq/proposed-digital-india-act.pdf
[8] What Is the Digital Twin Concept? How Does It Help an organization to Arrive at Better Decisions? Discuss the Sangam Digital Twin Initiative of Government of India, SPM IAS Academy (Mar. 2024)
[9] European Union. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, 2018 O.J. (L 303/59) (EU), https://digital strategy.ec.europa.eu/en/policies/non-personal-data.
[10] NITI Aayog, Responsible AI For All: Approach Document for India, Part 1 – Principles for Responsible AI (Feb. 2021)

[1] Authored by Poorna K (Reg.no: 126117023) Co-Authored by Harinibai.R (Reg.no: 126087013)
[2] Kaznah Alshammari, Thomas Beach & Yacine Rezgui, Cybersecurity for Digital Twins in the Built Environment: Current Research and Future Directions, J. Info. Tech. in Constr. (ITcon) Vol. 26, 159–173 (Apr. 2021)
[3] Cases of Digital Twins Across Industries, Tobler (Dec. 11, 2024), https://www.toobler.com/blog/digital-twin- use-cases
[4] What is the Digital Twin Concept? How Does It Help an organization to Arrive at Better Decisions? Discuss the Sangam Digital Twin Initiative of Government of India," SPM IAS Academy (Mar. 2024), https://spmiasacademy.com/mains_exam/q-9-what-is-the-digital-twin-concept-how-does-it-

help-an- organization-to-arrive-at-better-decisions-discuss-the-sangam-digital-twin-initiative-of-government-of-india
[5] India Digital Twin Market, Competition, Forecast & Opportunities, 2029 (Research and Markets, Oct. 2023), https://www.researchandmarkets.com/report/india-digital-twin-market
[6] About the 'Digital Twin: Sangam' Proof of Concept," Telecommunication Centre of Excellence (TCoE) India, https://sangam.tcoe.in/about
[7] Press Release, Press Information Bureau, "Sangam: Digital Twin Initiative of the Department of Telecommunications" (Apr. 1, 2024), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2032825
[8] Tejasvi Sharma, Digital Twins & Real-Time Monitoring: Transforming India's Infrastructure Lifecycle, EPC World (Oct. 2024), https://www.epcworld.in/digital-twins-real-time-monitoring-transforming-indias- infrastructure-lifecycle
[9] About EoI: Digital Twin – Sangam," Telecommunication Centre of Excellence (TCoE) India, https://sangam.tcoe.in/about-eoi
[10] Id
[11] Nitin Gadkari Unveils Digital Twin Strategy for Infrastructure, Geospatial World (Mar. 2024), https://geospatialworld.net/prime/business-and-industry-trends/nitin-gadkari-unveils-digital-twin-strategy- infrastructure
[12] Labanya Prakash Jena, Digital Twin: Making India's Clean Energy Architecture Versatile, Observer Research Foundation (Mar. 26, 2024), https://www.orfonline.org/expert-speak/digital-twin-making-india-s- clean-energy-architecture-versatile
[13] Muhammad Rashid et al., Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques, 17 Int'l J. Env't Research & Pub. Health 1, 5–6 (2020)
[14] Id at 6-8
[15] Id at 4
[16] Id at 9-12
[17] Smart-City IoT Architecture and Infrastructure Management Concepts, at 2–4
[18] Marija Kuštelega, Renata Mekovec & Ahmed Shareef, Privacy and Security Challenges of the Digital Twin: Systematic Literature Review, 30 J. Universal Computer Sci. 1782 (2024), https://orcid.org/0009-0004-7125- 5163
[19] NITI Aayog, Responsible AI #AIForAll: Approach Document for India, Part 1 – Principles for Responsible AI (Feb. 2021)
[20] National Data Governance Framework Policy, MeitY (26 May 2022)
[21] NDGFP, §§ 4.1–4.3; White Paper on Non-Personal Data Governance (2025)
[22] Craies on Statute Law (7th ed.) (principle of expressio unius est exclusio alterius)
[23] NDGFP, § 4.5 (classification of high-risk datasets including critical infrastructure).
[24] White Paper on NPD Governance (2025), at 7
[25] Regulation (EU) 2023/2854 (EU Data Act), arts. 4–12 (data access), arts. 23–29 (cloud switching), arts. 35– 38 (foreign government access).
[26] Kris Gopalakrishnan Committee Report on Non-Personal Data Governance (2020), at 24–29
[27] Proposed Digital India Act, 2023" (Digital India Dialogues, Mar. 9, 2023), Tata Consultancy Services (TCS) (pdf), https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/investor-relations/faq/proposed-digital-india- act.pdf
[28] Regulation (EU) 2023/2854, art. 3, Data Act (EU), Dec. 13, 2023, O.J. (L 2854) (entered into force Jan. 11, 2024).
[29] Id at Article 34
[30] Id at Article 14-21
[31] Id at Article 28
[32] Id at Article 6
[33] Id at Article 277
[34] Id at Article 33 read with Article 83 of Regulation (EU) 2016/679
[35] Kris Gopalakrishnan Committee Report, Non-Personal Data Governance Framework (2020)
[36] Id. at Chapters on Data Sharing Framework and Governance Structure.
[37] Id. at "Community Data" and "Data Trustee" Framework.
[38] Id. at Proposal for NPDA
[39] Non-Executive Think Tank on Digital Twin Strategy for Indian Infrastructure, Digital Twin Strategy for Indian Infrastructure (Geospatial Media & Communications 2025)