

"Code is Law" for IoT Data Sharing: Technical Architecture as Sovereign Enforcer in Commercial Data Sharing Platforms

Fjolla Berisha
Computer Science
Maynooth University
Maynooth, Ireland
fjolla.berisha.2024@mumail.ie

Leidiane Da Silva
School of Business
Maynooth University
Maynooth, Ireland
leidiane.goretedasilva.2021@mumail.ie

Peter Mooney
Computer Science
Maynooth University
Maynooth, Ireland
peter.mooney@mu.ie

Zohreh Pourzolfaghar
School of Business
Maynooth University
Maynooth, Ireland
zohreh.pourzolfaghar@mu.ie

Markus Helfert
School of Business
Maynooth University
Maynooth, Ireland
markus.helfert@mu.ie

Abstract - This paper examines how technical architecture enables data sovereignty over shared data, in commercial platforms, with a focus on the critical challenges posed by Internet of Things (IoT) data flows. Analysing four EU-based platforms (TomTom, Dawex, Skywise, Nallian) from the European Commission's 2018 study on business data sharing, we investigate how technical mechanisms operationalise sovereignty where contractual governance faces limitations of scale, speed, and complexity. Through cross-case analysis applying Lawrence Lessig's "Code is Law" framework, we identify distinct architectural enforcement patterns across the platforms. TomTom's API-centric model achieves preemptive control by terminating misuse in milliseconds, enabling real-time intervention. Dawex's blockchain-backed policy engine enables dynamic governance, translating licensing terms into executable cross-border constraints. Skywise's access silos structurally contain data usage, making unintended reuse architecturally implausible through purpose-bound design. Nallian's rights-granting engine delivers granular sovereignty, enabling field-level control. From these findings, we develop a four-mode Architectural Sovereignty Framework, conceptualizing enforcement mechanisms along two dimensions: timing (real-time vs. ex-post) and resolution (macro-level structural vs. micro-level granular). The framework identifies Preemptive, Adaptive, Structural, and Granular sovereignty as distinct modes through which code operationalises control in IoT data sharing contexts.

Keywords - Data Sovereignty, Data Sharing, Case Study, IoT, Code is Law

I. INTRODUCTION

The exponential growth of data generation, projected to reach 175 zettabytes by 2025 [10], has made data sharing essential for innovation. However, businesses face a fundamental tension: how to share data while retaining sovereignty (understood as sustained control over data usage) [38, 25]. The lack of data sovereignty poses diverse risks, such as loss of competitive advantage and unauthorised reuse [1], consequently leading towards eroded trust [2]. Data sovereignty, a cornerstone of the digital era, refers to the autonomy and capacity of individuals and organisations to exercise independent control and autonomy over their digital presence [38]. This encompasses their digital infrastructures, the technologies they employ, their raw IoT data, and all forms of digital content. At its core, data sovereignty is vital for

safeguarding the interests of all stakeholders within the thriving data economy [30]. It empowers businesses to dictate the terms under which their data is utilised, effectively treating it as a valuable economic asset [25]. This ensures that control remains with the data's owner, allowing them to make informed decisions about its access, processing, and storage, particularly in a globalised digital landscape [1, 38].

Data sharing, the transfer of data between entities, is now a key driver of innovation and value creation in the big data era, influencing product development and market competition [13]. Companies employ various strategies for this, broadly divided into one-way and two-way sharing [40]. One-way data sharing is straightforward: one company sells its data to another business [39]. In contrast, two-way data sharing involves companies exchanging data with each other, which can be a complete or partial exchange [40]. The goal of a two-way data sharing is to build a single market for data and give businesses access to high-quality resources. Reference [30] reveals that data sharing primarily happens within peer communities, comprising data experts from different companies [39]. These members who are part of peer communities, are united by shared interests or concerns, aiming to improve data exchanging practices [5, 12]. Each member acts as both a data consumer and provider.

Recognising the transformative potential of such practices, the European Commission's 2020 Data Strategy prioritises the free flow of data, highlighting its economic value, reusability, and role in innovation [39]. As a non-rivalrous good, data can be shared without losing value, making sharing key to maximising business benefits [5, 44]. Greater data availability is seen as vital for a competitive European data economy, aiming to better use public and private sector data [13, 42]. The Data Governance Act (DGA) and Data Act aims to boost private sector data sharing as well. The DGA creates a framework for voluntary sharing, fostering trustworthy data intermediaries and promoting data altruism for general interest [3, 38, 44]. Whereas the Data Act mandates access and sharing of industrial data from connected devices for consumers and businesses [3]. However, as [35] argues, the absence of clear data valuation procedures, due to data's unique nature compared to physical goods, creates uncertainty in data trading. This is further compounded by a lack of robust legal frameworks [37, 41], especially concerning intellectual property rights and liability for breaching terms of use [14]. Businesses worry that sharing data may hurt their

competitiveness, while Business-to-Business (B2B) data markets face information asymmetries and high transaction costs, often resulting in market failure [32, 44]. Formal data sharing agreements boost transparency and accountability by defining roles, purposes, and standards for data use, including confidentiality, intellectual property, and dispute resolution. However, they can be subject to interpretation and may not anticipate future challenges [3].

Authors in [25] emphasise that data marketplaces are unique because they must uphold data sovereignty and data provenance, ensuring data owners always retain control over their information, even when traded or processed [16, 11, 1]. According to [36], data colonialism arises when powerful private entities or states control other societies by imposing digital rules. To prevent such monopolies, discussions on data sovereignty are crucial, defining its meaning and rightful "sovereign." A democratic view emphasises individual digital self-determination, requiring smaller players and societies to collaborate in defending their sovereignty [25, 43].

Digital platforms like eBay, Uber, and Airbnb serve as crucial intermediaries, connecting two distinct groups of users, such as buyers and sellers, to facilitate transactions. They act as "matchmakers," drastically cutting down the time and effort users spend searching for what they need. These platforms also foster trust by mitigating information imbalances between parties [33]. While their exact internal data-sharing processes aren't detailed, their function inherently relies on the exchange of user data to enable their services [44]. According to [14], data brokers like Bloomberg, Oracle, Acxiom, and Nielsen gather massive amounts of data from various sources. They then sell these extensive datasets to other companies for uses such as marketing, identity verification, tracing people, and credit checks. Passenger data, including names, gender, age, and past booking history, is extensively shared via Computer Reservation Systems like Amadeus, Sabre, Mercator, and WorldSpan [40]. This information helps companies segment passengers, determine pricing, and target promotions.

Companies within the same industry sometimes share or pool data without direct payment. This often happens for purposes like credit referencing or fraud detection (e.g., sharing insurance claims data) [5]. Such data sharing occurs when there's a mutual commercial benefit and it doesn't stifle competition [13]. Companies sometimes provide limited, one-way access to their data, usually through APIs. This strategy is designed to encourage complementary innovation and grow their digital ecosystems [14]. However, the prevailing model, where data collectors like digital platforms maintain sole control over the data they gather, has sparked significant political and societal problems. These issues include privacy concerns, anti-competitive data practices, and public entities struggling to access crucial data from private firms [8, 6]. Seamless data flow across systems and organisations heavily on open interfaces and standardisation, which structure and centralise raw data for effective processing. According to [30], boundary resources like Software Development Kits and Application Programming Interfaces are crucial for data sharing/exchanging. To promote interaction and innovation, platforms use data marketplaces and communities [43]. Data sharing communities are often supported by an intermediary offering both organisational and technical assistance. According to [35], integrating blockchain into marketplace infrastructure is a key driver, enabling independent

transactions via smart contracts and boosting transaction integrity and data sovereignty.

Reference [29] provides a powerful lens for addressing data sharing complexities while upholding data sovereignty. It contends that in digital environments, technical architecture, what Lessig terms "code", regulates behavior more decisively than legislation, contracts, or market forces. In data sharing contexts, this manifests through three critical advantages: code preempts misuse through real-time interventions, embeds granular control at levels impossible in legal agreements [37], and scales governance across heterogeneous ecosystems [9]. As a result, this paper aims to answer: How do platform architectures ("code") operationalise data sovereignty in commercial data sharing? Through analysis of four EU-based platforms: TomTom (navigation data), Dawex (cross-sector marketplace), Skywise (aviation ecosystem), and Nallian (logistics community), we develop an Architectural Sovereignty Framework that identifies four distinct enforcement modes: Preemptive, Adaptive, Structural, and Granular Sovereignty, demonstrating how technical infrastructure implements and enforces governance principles established in contracts and policies, revealing that effective sovereignty in high-velocity IoT contexts requires engineering enforcement into data-sharing infrastructure.

II. METHODOLOGY

This study uses a qualitative case analysis of four commercial data-sharing platforms: TomTom, Dawex, Skywise, and Nallian, selected from the European Commission's 2018 case study report on B2B data sharing [13]. The methodology is designed to examine how technical architectures enforce data sovereignty in IoT contexts, applying Lawrence Lessig's "Code is Law" framework [29]. The four cases were deliberately chosen to reflect diversity in industry (mobility, cross-sector, aviation, logistics), data types (sensor streams, industrial datasets, telemetry, asset tracking), and enforcement mechanisms (APIs, blockchain, purpose-limited silos, rights engines). This variation enables exploration of how different architectures address sovereignty challenges such as velocity, granularity, and cross-border compliance. We also selected cases spanning [29] architectural enforcement spectrum: TomTom embodies preemption (real-time intervention), Dawex exemplifies adaptability (dynamic policy evolution), Skywise represents structural constraints (exploitation barriers), and Nallian demonstrates precision (sub-field governance).

To contextualise the cases, a literature review was conducted using targeted search queries combining "data sovereignty", "IoT data sharing," and the platform names. Inclusion criteria focused on peer-reviewed studies that reference at least one of the platforms. Key literature sources were used to validate and interpret the technical and governance mechanisms described in the case documentation.

Data collection was drawn from three main sources: primary EU case reports, platform technical documentation, and peer-reviewed analyses. Each case was analysed individually to identify how its architecture maps onto [29] modalities of constraint. A cross-case synthesis then highlighted recurring patterns and distinctive enforcement strategies across platforms.

III. TOMTOM- LESSIG: ARCHITECTURE > LAW

TomTom, a Dutch company specialising in navigation, traffic, and mapping products, has over 25 years of experience in business-to-business (B2B) data sharing [32, 12, 23]. A significant portion of its revenue comes from licensing IoT-derived traffic and location data like digital maps, real-time/historical traffic, and travel information. Their business model is primarily unilateral, focused on monetising [15] self-generated data [13].

TomTom operates as a privately-owned, hierarchical data marketplace that aggregates seller data to create tailored maps for customers [11, 36]. Its business model relies on direct customer relationships and bilaterally negotiated contracts, with a closed platform allowing TomTom to select participants [22]. Initially reliant on third-party data (i.e., licensing maps from TeleAtlas), TomTom acquired TeleAtlas in 2008 to gain control over data creation and updates [12]. This allowed cost-efficient, crowd-sourced map improvements and the development of proprietary traffic data layers, shifting away from external dependencies [7]. Their model is straightforward: users pay for the data delivered [23, 24]. Furthermore, TomTom uses a centralised cloud infrastructure for all data processing, from collection to distribution, ensuring data quality through internal review and protecting privacy via anonymisation [8, 25]. Its revenue is usage-based, with TomTom setting data prices. The company provides aggregated data through its customised map services, licensing maps, navigation software, and online services as application components, offering tailored solutions [13]. Payments are made in fiat currency [2, 34].

Primary users include automotive Original Equipment Manufacturers (OEMs), technology companies, Geographic Information Systems (GIS) providers, and large vendors, particularly for in-vehicle navigation, Advanced Driver Assistance Systems (ADAS), and autonomous driving [34]. Data is shared selectively with specific user groups under comprehensive licensing agreements, not openly (TomTom, 2025). These agreements define strict usage rights, re-use restrictions, and allow audits and legal action for breaches. All agreements explicitly prohibit sharing actual speed data with law enforcement [12].

A. Technical Mechanisms

Application Programming Interfaces (APIs) are the primary technical mechanism, chosen for safety, speed, and their ability to enable monitoring and rapid intervention against misuse (i.e., access suspension/termination). TomTom Maps APIs let developers integrate search, routing, mapping, traffic, and navigation features [13]. While data is sometimes shared via FTP, DVDs, or web portals, Application Programming Interfaces (APIs) are preferred for easy access, usage metering, and contract compliance verification [23, 24]. A limited-use Developer Portal allows demonstration access with strict modification prohibitions.

TomTom's deployment of APIs as its primary technical mechanism operationalises data sovereignty by enabling real-time monitoring and rapid intervention against misuse, including access suspension or termination. This architecture directly enforces contractual and regulatory boundaries by resolving third-party usage tracking difficulties, ensuring compliance through automated usage metering and immediate breach responses [24]. The limited-use Developer Portal further anchors sovereignty with strict modification

prohibitions, restricting demonstration access to pre-approved purposes [25]. While TomTom manages high collection costs through technological investments, it contends with unfair competition from entities allegedly non-compliant with European laws, underscoring sovereignty's dependence on equitable regulatory environments [22]. Critically, TomTom's operations rely on the EU Single Market's free movement principles for cross-border data collection and a clear legal framework for personal data and intellectual property protection [13], highlighting how technical controls (APIs) and regulatory foundations jointly safeguard data [12, 13]. TomTom exemplifies 'Code as Preemptive Regulation' [29] since its API architecture governs behavior in real-time, terminating misuse within milliseconds, demonstrating that code regulates faster and more decisively than law.

IV. DAWEX- LESSIG: ARCHITECTURE INTERPRETS LAW

Dawex, founded in 2015 by Fabrice Tocco and Laurent Lafaye, operates as a global independent third-party marketplace facilitating secure B2B data exchange and reuse [13, 22]. Dawex Systems SAS launched its active data marketplace in 2015 [35]. The platform connects companies seeking to sell data to potential buyers. The company presents itself as a "mix of eBay, Amazon, and Airbnb for data," functioning as a data marketplace that helps users anonymise datasets and offers license agreement templates [44].

Dawex operates as a neutral, third-party intermediary in a centralised two-sided platform, connecting data providers and buyers for B2B exchange [13]. It employs a hybrid market access model (supporting both selective and open participation) and functions cross-domain, primarily handling raw data with limited value-added services beyond data forwarding [22]. The platform manages legal and technical transaction aspects, including anonymisation and license templates, while generating revenue through transaction fees under a fixed-price model. Its architecture enables immediate processing and enhanced access control [45]. Businesses utilise Dawex when lacking resources to build proprietary platforms or when benefiting from its neutrality [42]. Dawex illustrates 'Code as Adaptive Law' [29]. Where static licensing agreements struggle with cross-border and multi-sector data flows, Dawex's blockchain-backed policy engine dynamically translates legal parameters into executable constraints, demonstrating code's superiority in adapting governance rules to evolving contexts [29, p. 236].

A. Technical Mechanisms

Dawex facilitates sharing of diverse data types, including customer, product, financial, and Internet-of-Things (IoT) data. Primary users span automotive, energy, agriculture, health, and retail sectors, encompassing startups, SMEs, and large enterprises. Data can be uploaded in formats like CSV, XLS, TXT, PDF, JSON, and GeoJSON [21]. Bulk data is encrypted for privacy. Dawex employs its own API to process requests, streaming data directly from suppliers to users while managing supplier-defined usage rights [22]. The platform includes search tools (filtering by sector, data type, geography, price) and offers visualisation (heat maps, tree maps) and sampling tools for pre-transaction assessment [13]. Dawex leverages distributed technologies like blockchain to reduce the need for external trust. This enables them to impose constraints on data users, maximising control over data usage

and minimising perceived risks for businesses involved in data sharing [3].

Companies must declare ownership rights during registration, with subscribers confirming legal authority to share company data [22]. Dawex never owns data and suppliers retain full control. Suppliers configure usage parameters (e.g., permitted sectors, re-sale rights, territories, duration), which align with legal conditions drafted by international IP/data lawyers [45]. Licensing agreements are customised based on these parameters and are negotiable. Dawex's step-by-step licensing framework prioritises speed, flexibility, and legal validity [13]. Authors in [10] highlight a key difference between Dawex and Terbine regarding metadata. Dawex allows data sellers to apply their own metadata, unlike Terbine, a prominent US-based, full-service data exchange, which imposes its own metadata layer on datasets.

V. SKYWISE- LESSIG: ARCHITECTURE PRE-EMPTS LAW

Airbus is a European multinational corporation that designs, manufactures, and sells civil and military aeronautical products [13, 17].

Skywise, a cloud-based data platform launched by Airbus in collaboration with Palantir Technologies in June 2017 (operational internally since 2015), is an open data platform designed to help airlines share aircraft data [40]. Skywise enables Airbus to better understand aircraft performance in real conditions, improve product quality, and develop new services [27, 28]. It allows airlines to assess their performance using Airbus data [18]. Designed as a win-win ecosystem, Skywise permits airlines to act as both data suppliers and users [31]. It is not a direct monetisation scheme for Airbus and participating airlines are not charged fees. Skywise supports data exchange among airlines, Airbus, and suppliers to enhance aircraft maintenance [12]. Such platforms may be open to qualified participants or close to specific partners [28]. Data can be pooled for mutual access or shared through secure, fast data spaces [44].

Typical datasets shared include onboard sensor data, components data, aircraft/fleet configuration, maintenance events, fuel consumption, and operational data like flight schedules [31]. Additional sources include operational interruption history, parts replacements, post-flight reports, and pilot reports [27]. While customer preferences are not currently shared (considered a potential future dataset subject to privacy rules), Airbus develops global benchmarks for fleet reliability and performance based on airline-supplied data, sharing these back with airlines for industry comparison [12]. Access is controlled via username/password, with each customer airline appointing an administrator to manage staff access and dataset permissions [6]. The platform is open to any aviation industry player. Airbus does not monetise Skywise through airline fees but uses it to improve products, offer new services, increase competitiveness, and ultimately sell more aircraft [17].

A. Technical Mechanisms

Built on the open-source Hadoop software framework, Skywise interoperates seamlessly with airlines' existing IT infrastructures, allowing easy data availability. It collects data from diverse sources and formats, processes and structures for analysis and visualisation [6]. Airbus works with original file formats, returning data through common tables and

visualisation tools [18]. Skywise is designed to ingest, clean, and model vast amounts of real-time IoT data from aircraft sensors. This includes diverse data types like time-series sensor data, structured operational and maintenance data, and unstructured technical documentation, all aimed at improving aircraft and services [4]. Airlines access and use data in three main ways: using visual analysis tools for reporting, utilising pre-built dashboards, and connecting their own analytics/development tools via APIs [13]. Most data transfers are automated, set up with customer IT departments, with upload frequency varying by data type and usage needs [26]. The Skywise platform offers "transparent, secured, and governance means" to integrate and structure diverse aviation data into a single Airbus Skywise Ontology. This ontology makes data visible, accessible, and understandable throughout an airline organisation [4]. Furthermore, according to [4], the platform features a highly granular and scalable access control system, enabling precise permissions for users and groups regarding data viewing and interaction within the organisation [12]. This robust control over data access is crucial for data sovereignty, ensuring data owners maintain control even when sharing information on the platform.

Despite its broad capabilities, Skywise is largely proprietary, which limits its compatibility with other systems and hinders wider industry adoption. Skywise illustrates 'Code as Structural Constraint' [29]. Rather than prohibiting raw data extraction through contractual clauses, Skywise's ontology-driven architecture makes such extraction technically impossible, proving that the most effective regulation is embedded in design, not documentation [27].

VI. NALLIAN- LESSIG: ARCHITECTURE REFINES LAW

Established in 2012, Nallian provides a cloud-based, customisable platform that enables business partners to collaborate more efficiently by sharing real-time data in a controlled, flexible, and agile environment [13, 14, 20]. Its core mission is to enable data-based collaboration, helping companies operate more efficiently as a community by overcoming fragmentation issues within a trusted environment [13, 19, 20]. Since 2012, Nallian has supported about a dozen business communities in Europe, with approximately 500 companies using its solutions by December 2016. Revenue is generated by enabling efficient data sharing. Nallian charges a flat fee for its data sharing technology, based on factors like user type, business connections, and applications, not dataset value. The company believes its platform offers indirect benefits by optimising processes and providing a comprehensive industry view [44].

A. Technical Mechanisms

Nallian offers a cloud-based data exchange platform, exemplified by its use in Brussels Airport's BruCloud data space [46]. This platform enables business partners to operate more efficiently as a community through controlled, flexible, and agile data sharing. Under the Data Governance Act (2019), such enablers are covered if they support commercial data-sharing relationships, providing the infrastructure for data transactions [3, 44]. The platform handles various data types including master/reference data, transactional data, and IoT streaming data, specific to each business sector and community. It operates with a core, cloud-based data sharing technology layer customisable per community [13]. This layer includes a community management tool facilitating user invitations to lower entry barriers. Nallian offers Software as

a Service (SaaS) platform layer, enhanced with value-added APIs and applications utilising a common data model to leverage stored data for insights [13]. Users integrate the platform into their systems, enabling automated data synchronisations and update notifications. Nallian's platform manages diverse data types, such as master, transactional, and streaming, binary, enabling datasets to be reused across multiple applications for community-wide insights. Its flat-rate pricing for data sharing technology is based on user type, connections, and applications, not dataset value [14].

Data can be injected via multiple methods: simple file uploads, API-based integrations, data pushed from connected devices, or B2B messages exchanged via Electronic Data Interchange (EDI) [13]. Crucially, data suppliers retain fine-grained control over data access and usage purposes through a rights-granting engine [41]. This allows suppliers to define roles and sharing rules down to the field level, including app providers [14]. The platform aids privacy compliance through features like data anonymisation and aggregation and offers data storage capacity for dataset retention and re-use by multiple applications, so that trust and security can be emphasised [33]. The company also emphasises granting data access while fully respecting usage rights [14]. Nallian's key of success is building trust by embedding granular access rights and roles in platform functionalities [13]. Nallian embodies 'Code as Precision Governance' [29]. Where legal language struggles to articulate field-level restrictions (e.g., 'share arrival time but not passenger identity'), Nallian's rights-granting engine executes this granularity natively, demonstrating that only architecture can achieve the resolution modern data ecosystems demand.

VII. ARCHITECTURAL SOVEREIGNTY FRAMEWORK

Our cross-case analysis suggests that technical enforcement of sovereignty in IoT data sharing can be conceptualised as a four-mode typology of architectural sovereignty. While [29] "code is law" highlights the regulatory role of architecture, our findings refine this into specific enforcement logics that platforms operationalise:

Preemptive Sovereignty: Code acts in real-time to monitor, meter, and terminate usage before contractual breaches occur. TomTom's API-centric model exemplifies this logic, where sovereignty is enacted through milliseconds-fast intervention [12, 13]. This mode addresses high-velocity IoT contexts where reactive audits are too slow.

Adaptive Sovereignty: Code dynamically translates contractual or policy parameters into executable constraints [21, 22]. Dawex illustrates this approach, where blockchain-backed policy engines evolve usage rules across jurisdictions and sectors [13]. Adaptivity matters most where cross-border governance or evolving terms of use are essential.

Structural Sovereignty: Code embeds constraints into the architecture itself, making misuse technically implausible. Skywise achieves this through ontology-driven silos and access tiers that structurally prevent raw data extraction [4, 17, 18, 12, 13]. Here, sovereignty is not just enforced but architecturally assumed, with exploitation foreclosed by design.

Granular Sovereignty: Code enables fine-grained, field-level governance, unachievable through language alone. Nallian's rights-granting engine embodies this mode, where suppliers can share, mask, or anonymise specific data

elements in real-time [13]. This addresses contexts where sensitive IoT attributes (e.g., speed vs. location) demand selective release [19, 20].

Taken together, these modes form an Architectural Sovereignty Framework (Figure 1), positioning enforcement mechanisms along two dimensions: *timing* (real-time vs. ex-post) and *resolution* (macro-level structural vs. micro-level granular). The framework reveals that sovereignty is not monolithic but enacted differently depending on platform design and data context.

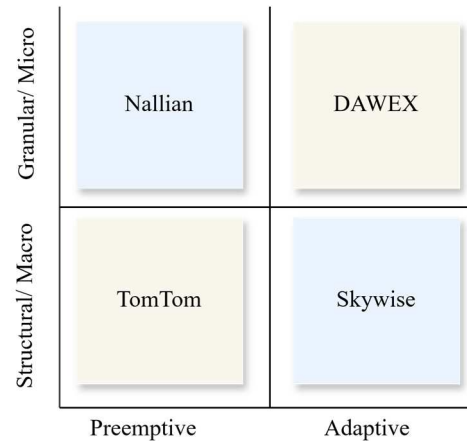


Fig. 1. Architectural Sovereignty Framework

VIII. DISCUSSION

Our analysis extends Lessig's [29] "code is law" framework to the domain of data sovereignty in commercial IoT data sharing, revealing how technical architecture operationalises control in contexts characterized by velocity, scale, and complexity. The Architectural Sovereignty Framework developed from our cross-case analysis identifies four distinct enforcement modes: Preemptive, Adaptive, Structural, and Granular, that demonstrate how technical mechanisms implement governance principles established in contracts and policies. The framework's contribution lies in conceptualizing architectural enforcement along two critical dimensions: timing (real-time vs. ex-post) and resolution (macro-level structural vs. micro-level granular). This typology reveals that sovereignty is not monolithic but rather enacted through different architectural logics depending on platform design and data context. TomTom's preemptive mode addresses temporal challenges through real-time intervention [13], while Dawex's adaptive mode enables policy evolution across jurisdictions [22]. Skywise's structural mode embeds constraints directly into system design [17, 18], and Nallian's granular mode achieves field-level precision [20]. These distinct modes suggest that effective sovereignty in IoT contexts requires selecting or combining architectural approaches based on specific governance requirements. Where contracts establish governance principles and define rights, technical architecture implements these principles at the operational level. This implementation is particularly critical in IoT environments where data velocity exceeds the temporal scope of manual oversight and data complexity surpasses the granularity of contractual language. TomTom's millisecond-response APIs operationalise licensing terms in real-time

[13], Dawex's blockchain-backed engines execute cross-border constraints dynamically [22], Skywise's ontology-driven design enforces purpose limitations structurally [17], and Nallian's rights engine implements field-level restrictions [20]. These mechanisms do not replace contractual governance but rather provide the technical means to enforce it at scales and speeds that IoT data sharing demands. The practical implication for platform designers is sovereignty-by-design: treating technical mechanisms (APIs, permission engines, access controls, cryptographic constraints) as primary governance infrastructure rather than mere implementations of legal requirements. For data owners considering sharing arrangements, the framework suggests evaluating platforms based on their architectural enforcement capabilities, whether they require preemptive intervention, adaptive policy evolution, structural containment, or granular control. For regulators, our findings indicate that data sovereignty mandates must extend beyond contractual requirements to specify architectural capabilities (e.g., real-time access revocation, field-level anonymization, audit trail generation).

Table 1 synthesizes the architectural sovereignty mechanisms across the four platforms, showing how each operationalises control through distinct technical approaches. The table maps platform characteristics (data type, technical mechanism) to their sovereignty enforcement mode, illustrating the diversity of architectural strategies for implementing data governance in IoT contexts.

TABLE 1. TECHNICAL ARCHITECTURE FOR IOT DATA SOVEREIGNTY IN COMMERCIAL PLATFORMS

Platform	IoT Data Type	Core Technical Mechanism	Sovereignty Enforcement
TomTom	Real-time traffic sensors	API-centric model	Preemptive termination of misuse
DAWE X	Industrial IoT streams	Blockchain policy engine	Dynamic cross-border constraints via smart contracts
Skywise	Aircraft sensor telemetry	Purpose-bound access silos	Structural containment of raw data
Nallian	Asset trackers/Warehouse IoT	Rights-granting engine	Field-level control

IX. LIMITATIONS

While this study demonstrates how technical architecture enables data sovereignty in commercial platforms, three key limitations warrant acknowledgment. First, the analysis focuses exclusively on European B2B use cases (TomTom, Dawex, Skywise, Nallian), limiting generalisability to non-EU regulatory contexts or consumer-focused models. Second, the "code vs. law" framework emphasises operational sovereignty but does not fully address power asymmetries, e.g., whether Small and Medium Enterprises can realistically enforce architectural controls against dominant players like Airbus. Third, the four cases prioritise platform-centric sharing; peer-to-peer or decentralised models (e.g., blockchain-based exchanges) remain underexplored. Fourth, our analysis relies on platform documentation and technical descriptions but lacks empirical data on actual enforcement

conflicts. We have no evidence of legal disputes involving these platforms, nor data on scenarios where contractual terms and technical architectures diverged. This limits our ability to empirically validate claims about the relative efficacy of code versus contracts in contested situations. Additionally, we do not examine the temporal dimension: while code can be rapidly modified (potentially undermining consistency), contracts require renegotiation and may prove more durable as governance instruments. The interplay between technical mutability and contractual stability warrants further investigation.

X. CONCLUSION

This study investigated four case studies in Europe. The analysis demonstrates that data sovereignty is fundamentally an architectural achievement. Through TomTom's preventive APIs, Dawex's dynamic policy engines, Skywise's purpose-bound silos, and Nallian's granular rights management, we observe [29] axiom, "code is law", manifested as technical governance. These platforms prove that sovereignty cannot be contracted retroactively but it must be engineered proactively into data flows. For practitioners, this necessitates prioritising sovereignty-by-design, treating APIs, cryptographic constraints, and permission engines not as technical accessories but as core governance infrastructure. Regulators must shift from compliance-centric mandates to certifying architectural capabilities (e.g., real-time revocation, field-level anonymisation). As data ecosystems grow in complexity, our findings extend Lessig's [29] 'code is law' thesis to the domain of data sovereignty. Where Lessig demonstrated that technical architecture regulates behavior in cyberspace, our cases reveal how architecture specifically enforces control over shared data.

ACKNOWLEDGMENT

This research was supported by the EnTrust project: Next Generation of Trustworthy Agri-Data Management, funded under the Marie Skłodowska-Curie Actions (MSCA) Doctoral Network as part of Horizon Europe (Grant Agreement No. 101073381).

REFERENCES

- [1] D.A.C. Assumpção and A. Blumenschein-Cruz, "Data sovereignty and international sovereignty principles - The data sovereignty observatory", 17th International Conference on Theory and Practice of Electronic Governance, pp. 388-391, December 2024. DOI: [10.1145/3680127.3680221](https://doi.org/10.1145/3680127.3680221)
- [2] R. Bergman, A.E. Abbas, S. Jung, C. Werker and M. de Reuver, "Business model archetypes for data marketplaces in the automotive industry: Contrasting business models of data marketplaces with varying ownership and orientation structures," *Electronic Markets*, vol. 32, pp.747-765, May 2022. DOI: [10.1007/s12525-022-00547-x](https://doi.org/10.1007/s12525-022-00547-x)
- [3] J. Bernal, "Private sector trust in data sharing: Enablers in the European Union," *Data & Policy*, vol. 6, pp. e30, August 2024. DOI: [10.1017/dap.2024.20](https://doi.org/10.1017/dap.2024.20)
- [4] W. Bernard and A. Hoffmann, "SKYWISE-Big data platform as a foundation of airlines predictive and health monitoring," 4th Asia Pacific Conference of Prognostics and Health Management, vol. 4, September 2023. DOI: [10.36001/phmap.2023.v4i1.3722](https://doi.org/10.36001/phmap.2023.v4i1.3722)
- [5] M. Botta, "Shall we share? The Principle of FRAND in B2B data sharing," *SSRN Electronic Journal*, April 2023. DOI: [10.2139/ssrn.4422925](https://doi.org/10.2139/ssrn.4422925)
- [6] B. Carballa Smichowski, "Alternative data governance models: Moving beyond one-size-fits-all solutions," *Interconomics*, vol. 54, pp. 222-227, October 2019. DOI: [10.1007/s10272-019-0828-x](https://doi.org/10.1007/s10272-019-0828-x)
- [7] M. Chen and J. He, "Research on the application of big data technology in government management," *IOP Conference Series: Materials Science and Engineering*, vol. 806, pp. 012001, April 2020. DOI: [10.1088/1757-899x/806/1/012001](https://doi.org/10.1088/1757-899x/806/1/012001)

- [8] P. Cichy, T.O. Salge and R. Kohli, "Privacy concerns and data sharing in the internet of things: Mixed methods evidence from connected cars," *MIS Quarterly*, vol. 45, pp. 1863-1891, October 2021. DOI: [10.25300/MISQ/2021/14165](https://doi.org/10.25300/MISQ/2021/14165)
- [9] R. D'Hauwers and A. Bourgeois, "Empowering data sovereignty: strategies of data intermediaries in data ecosystems," 37th Bled E-Conference: Resilience through digital innovation - Enabling the twin transition, pp. 243-256, May 2024. DOI: [10.18690/um.fov.4.2024](https://doi.org/10.18690/um.fov.4.2024)
- [10] M. De Saulles, "Data Liquidity: Data exchange platforms as drivers of innovation", March, 2020. DOI: [10.13140/RG.2.2.20887.93603](https://doi.org/10.13140/RG.2.2.20887.93603)
- [11] R. Eichler, C. Gröger, E. Hoos, H. Schwarz and B. Mitschang, "From data asset to data product—the role of the data provider in the enterprise data marketplace," Symposium and Summer School on Service-Oriented Computing, pp. 119-138, July 2022. DOI: [10.1007/978-3-031-18304-1_7](https://doi.org/10.1007/978-3-031-18304-1_7)
- [12] "Study on data sharing between companies in Europe - final report." European Union, Publications office, April, 2018, DOI: [10.2759/354943](https://doi.org/10.2759/354943)
- [13] "Study on data sharing between companies in Europe – case studies." European Union, Publications office, April, 2018, DOI: [10.2759/333340](https://doi.org/10.2759/333340)
- [14] A. De Streel and R. Feasey, "Data sharing for digital market contestability: Towards a governance framework," SSRN Electronic Journal, June 2021. DOI: [10.2139/ssrn.3855489](https://doi.org/10.2139/ssrn.3855489)
- [15] A. Shaji George and A.S. Hovan George, "Data sharing made easy by technology trends: New data sharing and privacy preserving technologies that bring in a new era of data monetization," *Partners Universal International Research Journal*, vol. 1, pp. 13-19, September 2022. DOI: [10.5281/ZENODO.7111123](https://doi.org/10.5281/ZENODO.7111123)
- [16] S. Gindl, "D3. 4 Data marketplaces with interoperability solutions I", 2020, Trusts [Online]. Available: <https://www.trusts-data.eu/wp-content/uploads/2021/01/D3.4-Data-Marketplaces-with-Interoperability-Solutions-I.pdf>
- [17] Airbus, "3 incremental packages – 3 levels of digital transformation", 2025, Airbus. [Online]. Available: <https://aircraft.airbus.com/en/services/enhance/skywise-data-platform/skywise-core-x>
- [18] API Tracker, "Skywise API", 2025, API Tracker [Online]. Available: <https://apitracker.io/a/airbus-skywise>
- [19] Nallian, "Nallian: Making the World Operate as One", n.d. Nallian [Online]. Available: <https://nallian.com/about-us>
- [20] Nallian, "Terms of use – Changi Air Cargo Community System (CACCS)" unpublished [Online]. Available: <https://cdn.nallian.io/shared/50c2ae3a-5420-4e62-8ab9-0171abf4901c%2Fpdf%2FCACCS%20Master%20Agreement.pdf>
- [21] Dawex Systems, "Data Exchange, Unleash the Full Potential of AI and Data", 2025 Dawex Systems [Online]. Available: <https://www.dawex.com/en/>
- [22] Dawex Systems, "Data Exchange Technology", 2025 Dawex Systems [Online]. Available: <https://www.dawex.com/en/data-exchange-technology/compliance/>
- [23] TomTom International BV, "Why TomTom", 2025 TomTom. [Online]. Available: <https://www.tomtom.com/>
- [24] TomTom International BV, "Documentation", 2025 TomTom website [Online]. Available: <https://developer.tomtom.com/documentation>
- [25] P. Hummel, M. Braun, M. Tretter and P. Dabrock, "Data sovereignty: A review," *Big Data & Society*, vol. 8, January 2021. DOI: [10.1177/2053951720982012](https://doi.org/10.1177/2053951720982012)
- [26] I. Jussen, M. Fassnacht, J.C. Schweihoff and F. Möller, "Reaching for the stars: Exploring value constellations in inter-organizational data sharing," 32nd European Conference on Information Systems, June, 2024. Available: https://aisel.aisnet.org/ecis2024/track10_dmds_ecosystems/track10_dmds_ecosystems/3
- [27] I. Kabashkin and V. Susanin, "Unified Ecosystem for Data Sharing and AI-Driven Predictive Maintenance in Aviation," *Computers*, vol. 13, pp. 318, November 2024, 318. DOI: [10.3390/computers13120318](https://doi.org/10.3390/computers13120318)
- [28] B. Kacar and E. Nalcacigil, "An examination of the usage areas of big data technology in civil aviation," *International Symposium on Electric Aircraft and Autonomous Systems*, pp. 109-115, December 2021. DOI: [10.1007/978-3-031-32639-4_15](https://doi.org/10.1007/978-3-031-32639-4_15)
- [29] L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books: New York, USA, 1999.
- [30] H. Lefebvre, P. Krasikov, G. Flourac and C. Legner, "Toward cross-company value generation from data: investigating the role of data sharing communities," 18th International Conference on Design Science Research in Information Systems and Technology, vol. 13873, pp. 33-49, May 2023. DOI: [10.1007/978-3-031-32808-4_3](https://doi.org/10.1007/978-3-031-32808-4_3)
- [31] I. Mancuso, A.M. Petruzzelli, U. Panniello, "Value creation in data-centric B2B platforms: A model based on multiple case studies," *Industrial Marketing Management*, vol. 119, pp. 1-14, May 2024. DOI: [10.1016/j.indmarman.2024.04.001](https://doi.org/10.1016/j.indmarman.2024.04.001)
- [32] B. Martens, A. De Streel, I. Graef, T. Tombal and D. Brown, N., "Business-to-Business data sharing: An economic and legal analysis", 2020, European Commission JRC 121336 repository [Online]. Available: <https://publications.jrc.ec.europa.eu/repository/handle/JRC121336>
- [33] N.R. Nodehi, F. Berisha, L. Da Silva, Z. Pourzolfaghar and M. Helfert, "Integrating cybersecurity, data sovereignty and trustworthiness in agri-data sharing environments: A conceptual framework," *IEEE 2024 Cyber Research Conference Ireland*, pp. 1-8, March, 2025. DOI: [10.1109/Cyber-RC160769.2024.10939388](https://doi.org/10.1109/Cyber-RC160769.2024.10939388)
- [34] A. Pagani, F. Bruschi and V. Rana, "Knowledge Discovery from car sharing data for traffic flows estimation," *IEEE 2017 Smart City Symposium Prague*, pp. 1-6, July 2017. DOI: [10.1016/j.urbmob.2023.100065](https://doi.org/10.1016/j.urbmob.2023.100065)
- [35] M. Spiekermann, "Data marketplaces: Trends and monetisation of data goods," *Interconomics*, vol. 54, pp. 208-216, October 2019. DOI: [10.1007/s10272-019-0826-z](https://doi.org/10.1007/s10272-019-0826-z)
- [36] M. Stürmer, J. Nussbaumer and P. Stöckli, "Security implications of digitalization: The dangers of data colonialism and the way towards sustainable and sovereign management of environmental data," 2021, arXiv:2107.01662v1 [Online]. Available: <https://arxiv.org/abs/2107.01662v1>
- [37] H. Ursic and B. Custers, "Legal barriers and enablers to big data reuse: A critical assessment of the challenges for the EU law," *European Data Protection Law Review*, vol. 2, pp. 209-221, December 2015. DOI: [10.21552/EDPL/2016/2/10](https://doi.org/10.21552/EDPL/2016/2/10)
- [38] F. von Scherenberg, M. Hellmeier and B. Otto, "Data sovereignty in information systems," *Electronic Markets*, vol. 34, February 2024. DOI: [10.1007/s12525-024-00693-4](https://doi.org/10.1007/s12525-024-00693-4)
- [39] M. Zieliński, "Business-to-Business data sharing within the EU digital market (2019-2021): Categorization of data and actors involved in data sharing operations", SSRN, May 2023. DOI: [10.2139/ssrn.4462295](https://doi.org/10.2139/ssrn.4462295)
- [40] H. Yu, Y. Gao and Y. Lu, "Company data sharing, product innovation and competitive strategies," *Expert Systems with Applications: An International Journal*, vol. 234, December 2023. DOI: [10.1016/j.eswa.2023.121083](https://doi.org/10.1016/j.eswa.2023.121083)
- [41] D. Zimmer, "Property rights regarding data?" *Trading data in the digital economy: legal concepts and tools*, pp. 101-108 November 2017 DOI: [10.5771/9783845288185-101](https://doi.org/10.5771/9783845288185-101)
- [42] H. Richter and P.R. Slowinski, "The data sharing economy: on the emergence of new intermediaries," *IIC-International Review of Intellectual Property and Competition Law*, vol. 50, pp. 4-29, December 2018. DOI: [10.1007/s40319-018-00777-7](https://doi.org/10.1007/s40319-018-00777-7)
- [43] T. Giese and R. Anderl, "Maintaining control over distributed data through a data sovereignty model," *IEEE Information Technology and Digital Applications*, pp. 1-7, November 2022. DOI: [10.1109/ICITDA55840.2022.9971218](https://doi.org/10.1109/ICITDA55840.2022.9971218)
- [44] L. von Ditfurth and G. Lienemann, "The data governance act: – Promoting or restricting data intermediaries?" *Competition and Regulation in Network Industries*, vol. 23, pp. 270-295, November 2022. DOI: [10.1177/17835917221141324](https://doi.org/10.1177/17835917221141324)
- [45] L. Belli, W. B. Gaspar, and S. Singh Jaswant, "Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries," *Computer Law & Security Review*, vol. 54, pp. 106017, September 2024. DOI: [10.1016/j.clsr.2024.106017](https://doi.org/10.1016/j.clsr.2024.106017)
- [46] BruCloud, "BruCloud Data Space," 2025 Brussels Airport Company [Online]. Available: <https://brucloud.com/>