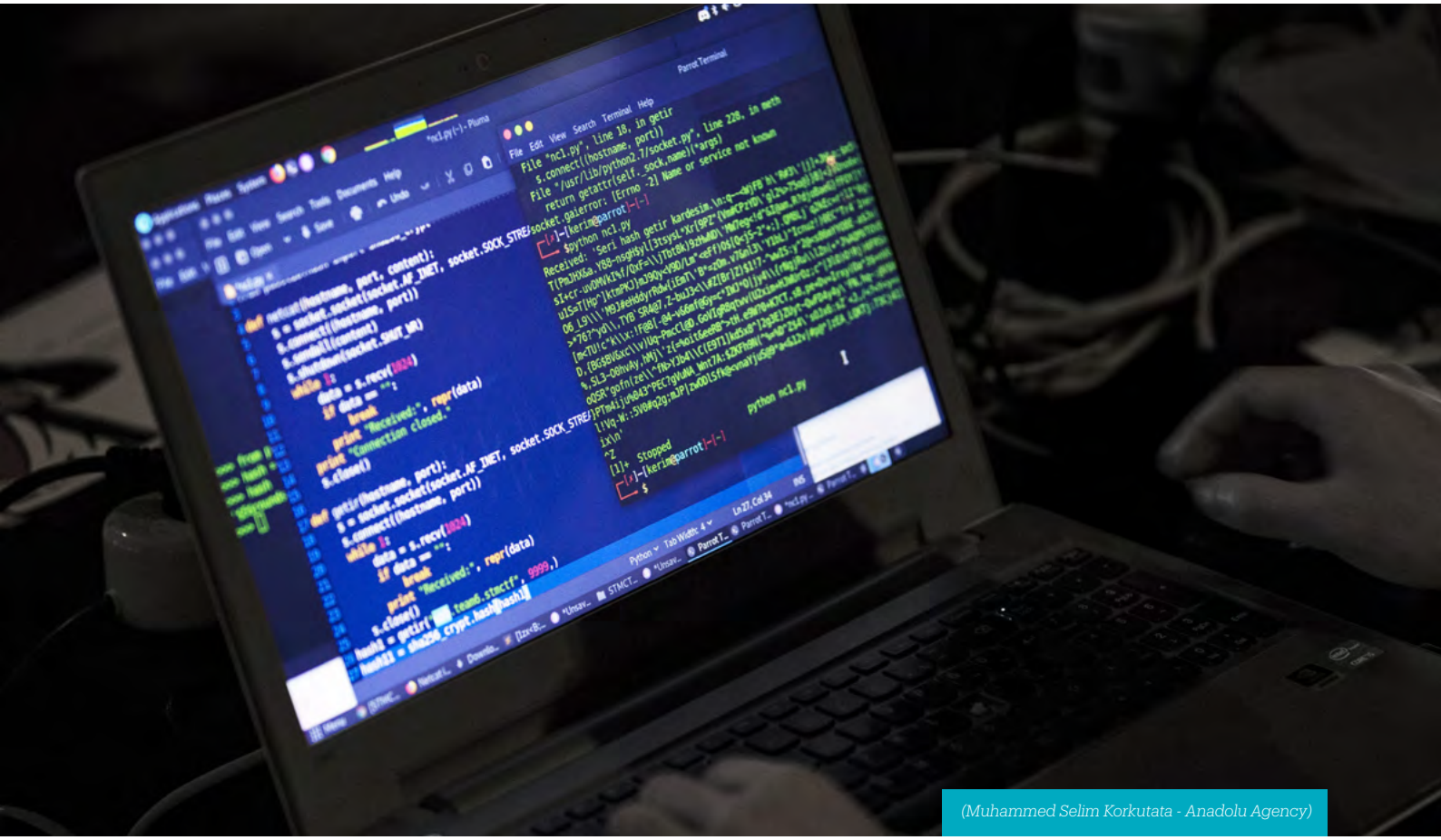
TRT WORLD research centre

Sovereign Data, Strategic Sectors: Why Healthcare and Automotives Are the New Frontlines

Şeymanur Yönt



(Muhammed Selim Korkutata - Anadolu Agency)

Data has evolved beyond a matter of privacy to become a core economic asset and a source of geopolitical power, elevating data localisation to a central policy tool in the global economy. As governments deploy localisation to strengthen control and strategic autonomy over data, companies face rising compliance costs and market entry barriers, while individuals experience shifting trade-offs between data protection and access to digital services. Against this backdrop, this policy outlook analyses the economic and geopolitical drivers of data localisation and offers targeted recommendations for both states and companies, with a particular focus on its growing impact on strategically sensitive sectors such as automotive and healthcare.

Data is a crucial asset for all: not only from a privacy perspective, but also as a source of revenue and strategic geopolitical power. Consequently, controlling data has become increasingly important in today's global economy, with data localisation serving as a significant tool towards that end. Countries are increasingly legislating data localisation rules with several outcomes: states acquire greater control over data for economic purposes while also strengthening their geopolitical positioning; companies face rising compliance costs and therefore higher barriers to market entry; and individuals enjoy greater privacy on the one hand but face limited access to certain services on the other.

This policy outlook first explains the nature of data localisation, uncovering the underlying primary economic and geopolitical drivers, and clarifies why these motivations, beyond the stated privacy concerns, must be taken seriously rather than treated merely as a compliance checklist. It then explains that, given their strategic, economic, and security relevance, two industries are likely to increasingly be subject to data localisation measures: automotive and healthcare. The policy outlook concludes with recommendations for states and companies, highlighting the often-overlooked risks behind the inclination towards data localisation.

1. Defining Data Localisation

There is no universally agreed definition of data localisation. However, most definitions concur that data localisation encompasses measures mandating the storage and/or processing of data within national territory. Divergences arise regarding the nature of the mandate and the scope of the practices covered. According to Cory and Dascoli (2021) and Svantesson (2020), data localisation includes implicit mandates such as restrictions on cross-border data flows, since these may result in more data being stored and/or processed locally. Conversely, López González, Casalini and Porras (2022) define data localisation as covering only explicit mandates on processing and/or storing data domestically.

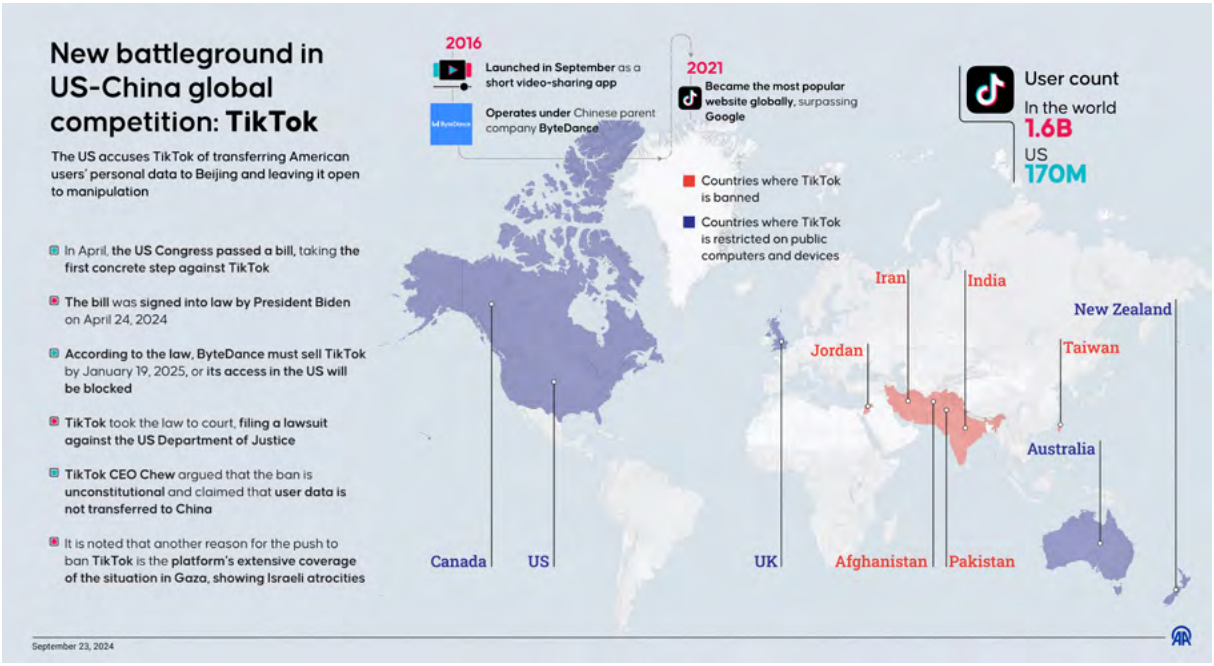
Regarding the practice of data localisation, while some definitions focus strictly on restrictions against not storing data locally, others include any conditions such as requirements for prior consent or standard contractual clauses for transferring data abroad. Chander and Lê (2015), for example, include taxes on the export of data within their definition of data localisation. Greenleaf, defining data localisation as measures that restrict other nations' control or sovereignty over data, identifies seven groups of measures: local copy requirements, local processing requirements, allowing data transfer subject to conditions, prohibition of data transfer, extra-territorial assertion or application of local privacy laws, and local representation requirements. This policy paper will consider the measures grouped by Greenleaf, as they better reflect the full range of motivations behind data localisation and are pertinent to the two industries analysed herein.

2. Data Localisation Drivers: A Focus on Economic and Geopolitical Motivations

As the definition of data localisation varies across the literature, the motivations for adopting data localisation measures also differ. The motivations include the legitimising motivation around data privacy and data protection concerns, as well as the underlying primary drivers of protecting national security, establishing data security, and developing domestic capacity through digital protectionism. The difficulty is in determining the real motivation behind data protection, since, usually, stated objectives – data protection and privacy concerns - do not match with the multiple and different ultimate geopolitical and economic objectives. For example, states may ultimately aim at furthering their protectionist digital industrial policies while asserting cybersecurity reasons for introducing data localisation measures. This is evident in France's efforts to promote a local data centre infrastructure by investing in local cloud companies and introducing a data tax. Between the lines, in fact, industrial policy and geopolitical ambitions, such as "building a France of digital sovereignty" and supporting domestic employment, are articulated at the state level.

In light of the French example, uncovering motivations behind data localisation measures is more important than it seems. Because first, data localisation is rarely a neutral privacy instrument. Rather, privacy frequently functions as a legitimising frame for measures primarily driven by industrial policy, economic protectionism, and strategic autonomy, which privacy-focused analyses fail to capture. For example, Eger (1978) suggested that data flow limitations within the EU, while primarily designed to protect privacy on paper, could serve as covert trade barriers intended to shield local economic interests from international competition. This aligns with President Charles Michel's speech, which highlights the centrality of digital sovereignty to strategic autonomy. By uncovering these hidden motivations, businesses can better navigate their commercial future.

Second, misreading the underlying motivations leads to flawed regulatory and corporate responses: when data localisation is treated merely as a compliance obligation,



states risk regulatory overreach while firms underestimate long-term operational, investment, and supply-chain risks embedded in data governance choices. For instance, in response to Russia's 2015 data localisation law (Federal Law No. 242-FZ), LinkedIn primarily saw the issue as a matter of regulatory compliance, maintained a wait-and-see approach, and communicated poorly with Roskomnadzor, Russia's data protection authority. This framing underestimated the broader political economy of the measure, which was entrenched in the state's desire to assert strategic control over data and digital platforms. Consequently, LinkedIn failed to anticipate that non-compliance would be met with severe enforcement rather than negotiated accommodation, ultimately leading to the complete loss of market access in Russia in 2016.

Third, data localisation increasingly operates as a geopolitical lever, intersecting with national security, digital sovereignty, and technological power, thereby extending its impacts well beyond domestic regulation into trade relations, cross-border data flows, and global digital fragmentation. Here, security rationales often function as an intermediate layer, translating geopolitical competition into regulatory action, while privacy remains the outward-facing justification. One of the most significant examples of this dynamic is the way the U.S. government has framed TikTok's data practices and ownership as a national security threat, culminating in legislation that requires ByteDance to divest TikTok's U.S. operations or face a nationwide ban. This illustrates how data governance and platform control are being used as geopolitical tools to limit a country's technological influence and protect another country's digital sovereignty beyond routine regulatory compliance. That's why businesses should also design their data frameworks with the day's geopolitics in mind.

The above examples show that data localisation operates within a hierarchy of intent: geopolitical control and industrial policy act as the primary drivers, while privacy is largely employed as a legitimising frame for underlying geopolitical and industrial targets. It reshapes competitive dynamics and dictates the terms of market access, favouring domestic industries. Ghana's effort to enact licensing requirements for the payment industry, requiring 30% local ownership and a Ghanaian CEO, is an example of how far such efforts can go. These and similar efforts may provide some advantages from an industrial policy perspective, including infrastructure stimulus, nurturing domestic champions, keeping high-quality data within borders, and facilitating easier auditing of digital transactions. Furthermore, data localisation can offer significant taxation benefits by resolving the jurisdictional complexities of taxing remote servers, a practice that often conflicts with established international taxation principles. By mandating local storage and processing, states can more effectively apply domestic tax laws to digital transactions and data-driven revenues, thereby eliminating the 'fiscal invisibility' of foreign-hosted services.

However, it is also likely to increase costs for SMEs, subjecting them to disproportionate entry barriers that stifle their ability to scale. Moreover, data localisation rules may act as a deterrent to foreign direct investment, resulting in an innovation gap and reducing domestic firms' access to advanced technology. Additionally, these rules may make a country's digital economy more vulnerable to physical disasters that could paralyse the digital economy and result in compounding financial losses. Nevertheless, the rationale behind these measures often extends beyond economic concerns, as states increasingly prioritise geopolitical competition and strategic control, with privacy considerations becoming secondary.

Rising strategic competition, concerns over technological dependence, and the securitisation of data led to the adoption of data localisation as a precautionary measure to address geopolitical concerns, maintain regulatory control, and signal sovereignty. As a natural outcome of this, the economic efficiency costs traditionally associated with localisation are increasingly treated as secondary considerations, surpassing privacy concerns but remaining subordinate to strategic autonomy, as states prioritise strategic autonomy over short-term market integration, reinforcing the persistence and expansion of data localisation measures. For instance, the EU's backing of the Gaia-X initiative reflects the collective effort to reduce technological dependence on U.S. and Chinese cloud providers, with the aim of signalling its 'digital sovereignty'. This and similar initiatives may, on the one hand, provide strategic autonomy, protection against foreign surveillance, and help countries assert digital sovereignty; while on the other hand, they may result in domestic surveillance, fragmentation of the internet, diplomatic tensions and retaliation, and a higher risk for cyberattacks due to geographic concentration of data. For example, China's National Intelligence Law grants authorities broad access to data without judicial oversight. Consequently, data localisation requirements make it significantly easier for the government to retrieve and monitor information. Ultimately, as data becomes synonymous with strategic and economic power, these geopolitical and economic motivations are converging upon high-stakes sectors such as healthcare and automotives, where the sensitivity of information signals even more stringent localisation measures that are likely to be enacted.

3. Two Industries and Divergent Logics of Sovereignty: Data Localisation as Real-Time Tactical Security vs. Long-Term Structural Autonomy

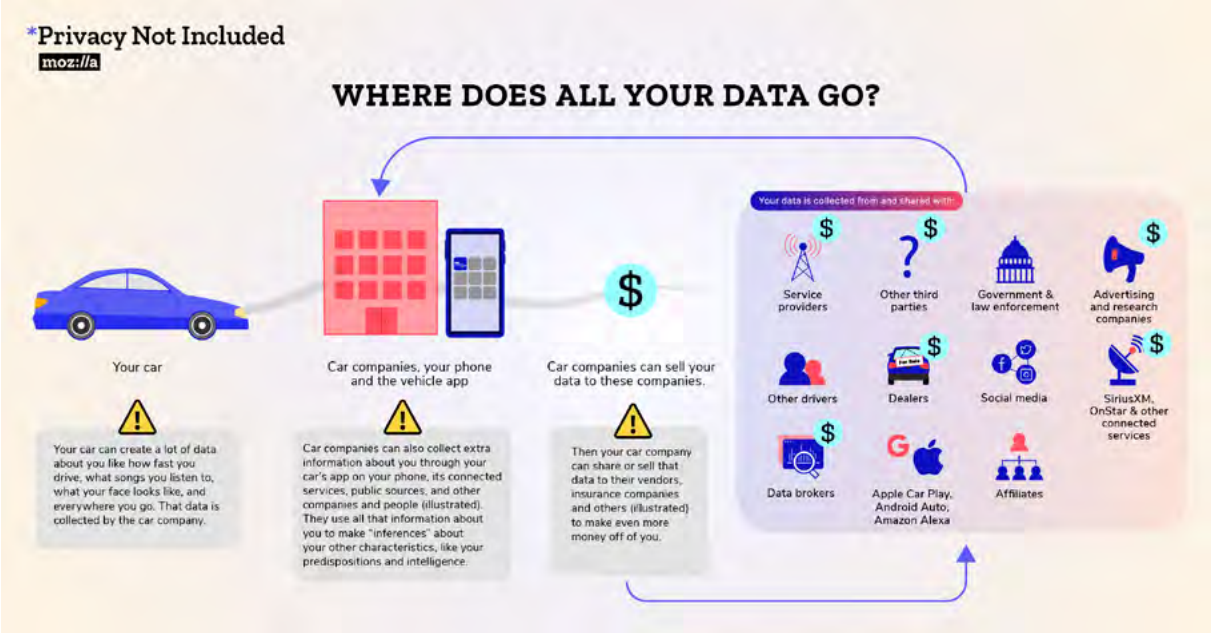
Given their political and economic value and the significance of the data they generate, the automotive, especially autonomous car, and healthcare industries, including pharmaceuticals and medical devices, are likely to be increasingly targeted by data localisation measures. However, these sectors reflect distinct logics of sovereignty, which in turn shape the data localisation policies targeting each industry and necessitate a nuanced policy response that accounts for these differences. The automotive industry is driven by a forward-looking focus on real-time data, providing a significant technological edge through AI model training, mapping, and system optimisation. Simultaneously, this data creates a tactical security edge, as the high-resolution mapping information involved grants immense surveillance capabilities to any state or entity that can access it. By contrast, healthcare data localisation is rooted in a custodial and biopolitical logic concerned with long-term structural sovereignty. Rather than securing real-time movement, it focuses on the governance of population-level data to enable predictive health policies and safeguard biological security, thereby preventing strategic dependencies by ensuring domestic control over R&D, patent development, and biotechnological supply chains.

These divergent logics of sovereignty result in contrasting regulatory frameworks for data localisation. In the automotive sector, this manifests as edge-focused, hardware-centric mandates that prioritise the localisation of on-board processing and sensor data to mitigate immediate tactical risks. In the healthcare industry, however, the focus shifts to cloud-based and jurisdictional frameworks that mandate the use of sovereign cloud infrastructure to ensure the long-term security of the data repository and its immunity from foreign legal reach.

3.1 Automotives Industry

Automotives already collect vast amounts of data, but with advancements in technology, increased connectivity, and the rise in popularity of electric, autonomous, and semi-autonomous vehicles, the volume of data is growing rapidly. As automotives become more technologically advanced with integrated services and sensors, the scope of data collected expands beyond gestures, call logs, location data, driving behaviour data, driver identity data and includes super intimate, to include extremely sensitive information such as medical and genetic data. Furthermore, autonomous and semi-autonomous vehicles not only collect data on drivers but also gather geographic information about roads, which often raises security concerns for states. It is important to note that data collected by automotives includes not only raw data but also information inferred from it and used by car companies. According to research by the Mozilla Foundation, 23 of the 25 car companies surveyed draw inferences from the data they collect, and 9 of them openly state that they might sell this data to third parties.

This illustrates how data is used not only to operate services and generate direct revenue for business owners, but also to create indirect revenue streams through its monetisation and sale, reflecting the economic value of the data in the automotive sector. Indeed, it is estimated that by 2030, the monetisation of data collected from vehicles could constitute an industry worth up to USD 750 billion, reflecting the rapid expansion of secondary markets built around automotive data that extend well beyond core vehicle services. A growing ecosystem of automotive data brokers illustrates this trend. For example, "vehicle data hubs" such as High Mobility publicly advertise extensive portfolios of data products collected through commercial partnerships



Source

with car brands, including precise geolocation data, biometric indicators such as heart rate, driver fatigue metrics, and dozens of additional data categories.

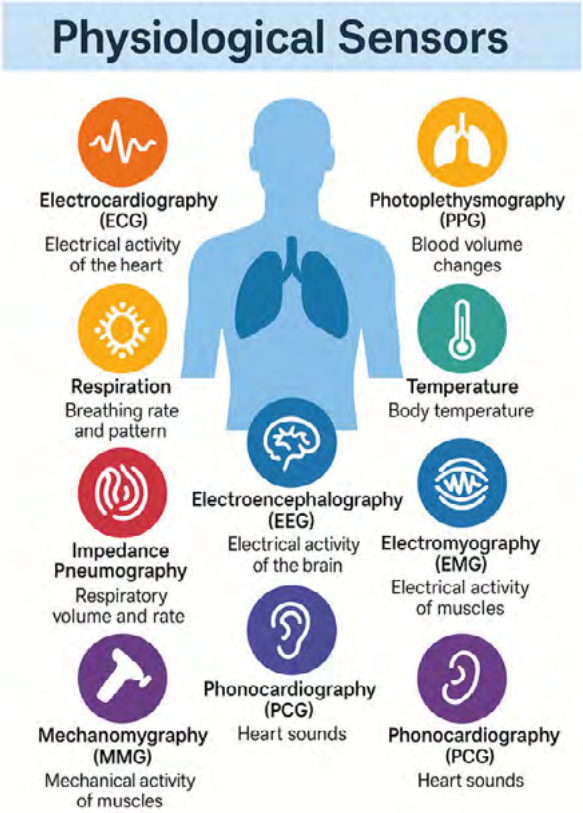
However, the value of the data collected goes beyond its commercial potential; the depth and granularity of automotive data also transform it into an important strategic asset with significant geopolitical implications. From a geopolitical perspective, the ability to track movement and monitor citizen health through automotives provides countries with unprecedented capabilities for domestic surveillance and strategic intelligence gathering. For example, high-resolution geolocation data allows foreign entities to map sensitive military locations, government facilities, and the movement of strategic personnel, while the ability to monitor driver behaviour and biometric health indicators provides a detailed level of insight into a population's daily life, which can be weaponised for social engineering or mass surveillance by state actors. The U.S. BIS Connected Vehicles Rule, prohibiting VCS Hardware Importers' and Connected Vehicle Manufacturers' engagement in certain transactions involving VCS hardware and software, and ADS software connected to Chinese or Russian-affiliated companies, underscores the importance of the data collected in the industry from a national security perspective.

Given the economic value and strategic importance of data in the automotive industry, it is reasonable to expect data localisation measures to increasingly target the sector. China has already enacted enforceable regulations, the Provisions on the Administration of Automobile Data Security (for Trial Implementation), limiting the transfer of Auto Data, requiring local data storage in China unless export of important data is necessary and a security assessment is conducted. In line with this, China, targeting the industry, banned Tesla cars from entering military complexes and housing areas for personnel employed in sensitive industries and state agencies.

Given the data's sensitivity and significance, the automotive data ecosystem is likely to face increasing localisation requirements, both on security grounds and as part of broader efforts to shape market outcomes and retain data-driven value within national economies. This trend will not be limited to China; similar regulations are increasingly expected to restrict data flows involving critical infrastructure, national security, and grid stability, as well as sensitive personal data, making on-board processing a mandatory requirement rather than relying on global cloud servers. Such measures are likely to manifest as sophisticated technical mandates, including the prohibition on exporting raw sensor data, whereby high-resolution LiDAR and camera feeds must be processed at the 'edge' within the vehicle, and the establishment of sovereign mapping gateways that ensure HD map data remains under domestic control. Furthermore, states may introduce mandatory local AI training requirements, forcing foreign manufacturers to decouple their global learning models and anchor their R&D infrastructures within the host country to access domestic driving data. This transition from simple residency to hardware-centric and algorithmic localisation reflects a dual-purpose strategy: neutralising immediate kinetic security threats while simultaneously forcing the relocation of the high-value digital supply chain to domestic borders. This, in turn, necessitates a more proactive and coordinated approach by both states and private actors in managing data localisation.

3.2 Healthcare Industry

The healthcare industry, especially pharmaceuticals, MedTech, and HealthTech, is another sector that collects vast amounts of personal data, much of which is highly sensitive. With the proliferation of IoT products, telehealth systems, and increased use of AI, the significance and volume of data collected has grown substantially. Connected devices, wearable health monitors, telehealth platforms, electronic health records, and AI diagnostic tools continuously generate detailed personal data, including temperature, blood volume changes, and electrical activity of the brain. These technologies, while improving access and care quality through, for example, anomaly detection, also exponentially expand the scale of health information collected across networks of providers and third-party services.



Source

The nature and the amount of data collected naturally raise privacy concerns. Healthcare data inherently contains the most sensitive categories of personal data, such as medical diagnoses, treatment plans, genetic information, and even behavioural health indicators. The integration of IoT devices and AI systems that continuously collect and transmit data, often across multiple platforms and stakeholders, heightens data sensitivity, intensifying privacy concerns. Countries with privacy concerns at stake, attach greater importance to regulating healthcare data, through introducing stricter requirements for transferring the data abroad, as a form of data localisation.

But beyond that, the collected data offers a significant revenue opportunity for companies, especially through analytics services, AI-driven predictive modelling, or partnerships with pharmaceutical, research, and insurance firms seeking patient stratification and real-world evidence. A report by EY (2019) found that the NHS data has a valuation of several billion pounds and a realisation of £9.6bn per annum in benefit (NHS benefit and patient benefit combined). The scale of the opportunity provided by health data is further evidenced by the rapid growth of the global digital health market, which is expected to reach a revenue of approximately USD 177.7 billion in 2026, with a significant portion of this value derived from data-intensive segments like Digital Treatment and Care. This expansion highlights how health-related information is no longer just a clinical record, but a cornerstone of a massive, data-driven economic ecosystem.

Moreover, while privacy remains the primary legitimising frame for regulation, the significance of health data extends far beyond individual protection; it has fundamentally evolved into a strategic lever for geopolitical control and a cornerstone of industrial policy. The concerns around national security and geopolitical strategy of the healthcare data include the use of large healthcare datasets for genetic surveillance and societal control, exerting leverage, developing bioweapons, dominating the industry, and creating drug and treatment dependencies on other states. That's why the U.S. National Counterintelligence and Security Center classified Chinese worldwide collection of healthcare data as a threat to national security. According to the NCSC, the purpose of low-cost DNA tests and COVID-19 kits marketed by the companies such as BGI Group is creating a global genomic database.

These concerns inevitably drive a growing inclination toward data localisation across the healthcare sector. For instance, several jurisdictions such as GDPR of the EU classify healthcare data as sensitive data, which is subject to stricter regulations for processing, including transfer abroad. As a result, even though there are no official EU requirements to store healthcare data locally, since data transfers are subject to several conditions, most companies prefer to keep the data within national borders, as a form of de facto data localisation. Similarly, Australia requires information relating to health records to be stored and processed within its borders unless the records do not include "personal information in relation to a healthcare recipient or a participant in the My Health Record System" or "identifying information of an individual or entity". In Japan, the Guidelines on Security Management of Information System and Services Handling Medical Information requires that information systems for the handling of medical data must be located in the territory of Japan. On the other hand, South Korea obliges cloud servers storing patient electronic medical records created by hospitals to be situated within its borders.

It is reasonable to expect this trend to persist and further intensify over time. In this context, it would not be unreasonable to say that the requirements governing cross-border transfers of sensitive personal data, particularly healthcare data, will become more stringent, shifting from simple residency rules to comprehensive jurisdictional mandates. Likewise, it is also possible to expect an increase in regulations concerning the use of sovereign cloud infrastructures. Already, France showcased one of the most proactive examples of digital sovereignty in the healthcare sector through its cloud certification regime (SecNumCloud certification regime), administered by the French National Cybersecurity Agency. While SecNumCloud itself is a cloud security framework, its latest iteration includes stringent requirements, for example data residency and legal immunities from extraterritorial laws like the U.S. CLOUD Act, that effectively shape how sensitive health data can be hosted and processed. By mandating that data be stored within infrastructures immune to foreign subpoenas, France is not merely protecting privacy; it is asserting a biopolitical sovereignty that ensures the state remains the sole custodian of its citizens' biological information.

This regulatory pressure has led global technology providers to establish strategic partnerships with French companies, such as Microsoft's Bleu sovereign cloud initiative with Orange and Capgemini, and Google Cloud's collaboration with Thales under S3NS, to create cloud environments capable of securing healthcare data under exclusive French and European jurisdictional control. Moreover, as AI gets to the centre of diagnostics, governments started to realise the competitive advantage provided by the healthcare data in training AI models. Consequently, new regulations may start to specifically target the secondary use of data to prevent 'data harvesting' by foreign entities and to secure domestic control over the future of biotechnological innovation. Considering these, the trend toward formal and informal data localisation, driven by the need for long-term structural autonomy, is likely to accelerate; and therefore, countries and enterprises must enhance their readiness to navigate these evolving regulatory requirements.

4. Recommendations for States

While data localisation has legitimate economic and security concerns behind it, blunt data localisation often translates into unintended negative outcomes. Such restrictions carry the risk of resulting in weaker security measures because local providers face less competitive pressure to invest in advancing their services, making such systems easier targets for foreign surveillance. Similarly, restrictions on transfer of potential cybersecurity threats ('threat data') may lead to increased vulnerabilities and lowered resilience. Moreover, centralising data makes that infrastructure more attractive target for both criminal hackers and foreign intelligence agencies. From a privacy standpoint, the effectiveness of these measures against foreign access is questionable; however, they significantly simplify domestic surveillance by placing personal data under the immediate jurisdiction and control of the government.

From an economic perspective, data localisation harms development by increasing costs for businesses denied access to global services, reducing consumer choice, hampering start-ups dependent on foreign platforms, preventing access to cloud computing innovations, impeding Internet of Things development, and restricting big data analytics, while providing minimal employment benefits as data centres are capital-intensive, with few workers and mostly imported equipment. Cory and Dascoli's economic model shows that a one-unit increase in the data restrictiveness index reduces gross output traded by 7%, decreases productivity by 2.9%, and increases prices by 1.5% cumulatively over five years. Notably, China, Indonesia, Russia, and South Africa experienced measurable economic costs from increasing data restrictions between 2013–2018, with South Africa suffering the largest marginal losses (a 9.1% reduction in gross output). Another model suggests significant GDP impacts, such as a 1.7% decrease for Vietnam and 1.1% for the EU under certain scenarios based on proposed regulations. Moreover, data localisation significantly hinders medical research and technological innovation by fragmenting the global datasets necessary for large-scale AI training and clinical trials. Finally, research indicates that preventing a slide into 'data nationalism' is six times more valuable than merely liberalising existing restrictions, representing a potential impact equivalent to 0.37% of the EU's GDP. This underscores that data localisation measures act as significant deterrents to economic output, with the costs of new restrictions far outweighing the benefits of current trade agreements.

Despite its inherent challenges, data localisation provides strategic benefits that policymakers must negotiate within an increasingly fragmented global order. One of the most important practical advantages is the simplification of regulatory and law enforcement access to evidence, since existing international mechanisms such as Mutual Legal Assistance Treaties (MLATs) are documented as outdated, complex, and slow, with some requests taking 10 to 18 months to fulfil. By mandating local storage, governments bypass these international backlogs, ensuring that information relevant to criminal investigations is immediately subject to domestic warrants and available for inspection by local authorities. Furthermore, exclusive data storage with local companies that have no legal presence abroad or "nexus" in foreign jurisdictions can effectively shield information from lawful access requests and intelligence surveillance in those jurisdictions. Recognising that states may prioritise these strategic imperatives and addressing their geopolitical concerns over global economic efficiency, the following recommendations do not represent a theoretical 'best practice' for a borderless internet. Instead, they offer 'second-best' strategies aimed at manag-

(Necati Aslım - Anadolu Agency)

ing structural constraints, designed to help states achieve their geopolitical objectives while minimising the inevitable economic and technological friction.

To mitigate risks associated with data localisation while addressing legitimate concerns, states should adopt a more nuanced, "carrot-based" approach focused on value creation rather than mere restriction. For those purposes, states should:

- **Prioritise Interoperability**

Since universal liberalisation is often politically unfeasible in the current geopolitical climate, instead of pursuing universal harmonisation, which often clashes with differing state value systems, or accepting a fragmented and expensive digital landscape, the focus should shift toward creating interoperable data localisation standards. Policies towards interoperability may include:

- Supporting early research and discussions about potential best practices
- Conducting joint pilot projects and regulatory sandboxes to test potential regulation
- Cooperating in cybersecurity protections
- Adopting international protocols (such as ISO/IEC) and APIs to enable data to move across applications and jurisdictions without manual intervention, and modernising principles like MLATs
- Developing financial oversight frameworks that focus on regulatory reach rather than where data is stored
- Signing Digital Economy Agreements to establish binding rules on cross-border data flows, digital trade, and emerging technologies, or being part of the APEC Cross-Border Privacy Rules (CBPR) System, which facilitates legally and practically easier personal data transfers
- Harmonising government access principles

- **Implement a Tiered Functional Separation**

Acknowledging the inevitability of state intervention, states should avoid "absolute" localisation, which risks isolating the domestic tech ecosystem. Instead, a tiered regulatory regime is a must:

- **Tier 1 (National Security & Critical Infrastructure):** High-sensitivity data (biometrics, precise geolocation, vehicle-to-infrastructure logs) may remain under strict local jurisdiction to avoid the reach of other states. This way, countries may protect these data from the laws in other countries, such as the U.S. PATRIOT Act, which grants U.S. law enforcement agencies broad authority to access data stored by U.S.-based companies, regardless of where the servers are physically located.
- **Tier 2 (Commercial & Behavioural Data):** This tier should allow cross-border transfer provided an

adequate level of protection in another jurisdiction and a local copy (mirroring) is maintained, or laws requiring data to be made available to authorities without delay, regardless of where it is physically held, to ensure regulatory oversight and domestic availability.

- **Tier 3 (Anonymised & Derived Models):** To foster innovation, processed models and anonymised sets should flow freely, ensuring domestic firms remain integrated into the global AI R&D pipeline.

- **Turn "Data Storage" to "Value Extraction"**

A "passive storage" model turns a country into a mere digital warehouse. To acquire the economic benefits behind data localisation purposes, states should transform localisation into a proactive competition tool by conditioning data access on value-added obligations:

- **Voluntary Local R&D**: Incentivise global firms with tax reliefs and R&D subsidies to perform model training and software development within local data centres.
- **Technology Transfer**: Encourage partnerships between global giants and the domestic ecosystem in high-tech fields like battery optimisation, autonomous sensors, and telehealth AI.
- **National Data Pools**: Establish state-governed, standardised data pools. By granting local startups and SMEs preferential access to these pools, states can lower innovation costs and create economies of scale in sectors such as urban planning and preventive medicine.

5. Recommendations for Companies

In an era where data is increasingly viewed as a sovereign asset, companies must move beyond viewing localisation as a mere compliance burden. Rather than resisting an irreversible geopolitical trend, firms should treat localisation as a structural constraint that requires a strategic pivot. Instead, it should be integrated into the core business strategy as a marketing asset that signals domestic security and trust. Organisations should assess localisation risks during the initial market entry and investment planning phases, ensuring operational adaptation, technical resilience, and proactive legal compliance rather than attempting to retrofit systems after deployment. Accordingly, companies should:

- **Architect for "Localisation-by-Design"**

To operate effectively within a fragmented digital economy, companies should adopt modular data architectures from the outset.

- **Modular Infrastructure**: Instead of a monolithic global cloud, firms should implement regional data lakes and modular storage. This ensures that demands for local "mirror servers" can be met with minimal operational disruption.
- **The Tesla Model**: A prime example of this "early adaptation" is Tesla's Shanghai Data Centre. To comply with regulatory requirements, Tesla established a local facility in 2021 to store all operational data generated in China. By proactively committing to local storage, Tesla transitioned from a scrutinised foreign actor to a compliant market leader.

- **Ensure Technical Resilience and Data Security**

Empirical data underscores the strategic value of data protection, as approximately 55% of businesses anticipate a surge in sales driven by the increased consumer trust that robust safeguards provide. While the benefits vary by regulatory approach, open safeguards are perceived to offer the highest marginal gains, potentially increasing sales by 13.5%, compared with 12.5% for pre-approved safeguards. These findings suggest that when companies move beyond viewing localisation as a mere compliance burden and integrate it as a trust-building marketing asset, they can effectively offset operational costs through enhanced market reputation and customer loyalty. Accordingly, to avoid data localisation costs and enjoy the benefits akin to higher trust, companies should:

- Employ end-to-end encryption and anonymisation technologies to prevent unauthorised access.
- Focus on logical access controls and robust cybersecurity maintenance, which are more effective at preventing breaches.
- (if possible) Use sharding, i.e., storing different pieces of a database across multiple global servers, to ensure no single location holds enough data to re-identify individuals, thereby enhancing privacy

- **Leverage "Data Trusteeship" and Local Alliances**

As a pragmatic response to restrictive regimes, companies must establish trust, effectively shifting the narrative from 'data extraction' to 'ecosystem participation.

- **Data Trusteeships**: Companies should develop trusteeship arrangements with local technology partners. This ensures that data is governed under local jurisdictional control, mitigating geopolitical friction.
- **Controlled Data Sharing**: By engaging in public-private partnerships to share anonymised data for smart city planning, traffic safety, or insurance, companies position themselves as "infrastructure providers" rather than "data miners." TikTok's partnerships with local entities to manage regional data flows serve as a contemporary model for building political legitimacy through shared control.

(Tayfun Coşkun - Anadolu Agency)

- **Use Local Data Processing as a Bargaining Chip**

Companies can use local AI model training as a powerful tool in industrial diplomacy, keeping in mind that true value lies in processing, not just storing, data. Offering to perform high-value AI model training and complex analytics within national borders allows companies to trade 'computational sovereignty' for market access.

  - **Knowledge Transfer**: Committing to train high-value analytical models within the host country generates local intellectual capital, know-how, and employment. This transforms a data centre investment into a strategic contribution to industrial policy, making market access a mutually beneficial "trade" rather than a concession.
  - **Federated Learning**: To maintain global model integrity without breaching sensitive borders, firms should deploy federated learning, a decentralised machine learning technique where the algorithm is trained across multiple local servers holding local data samples, without ever exchanging them. This ensures high-precision results and continuous innovation while strictly adhering to localisation mandates, effectively decoupling the utility of data from its movement.

- **Transition to Data-Based Service Models**

As cross-border flows of raw data become restricted, the revenue model must shift from "selling data" to "delivering data-driven services."

  - **Service-Centricity**: Companies should focus on selling outcomes, such as predictive maintenance, dynamic insurance, or fleet optimisation, via controlled API access. When a service is sold, the physical location of the raw data becomes secondary to the value it produces.
  - **Pricing Data Portfolios**: Firms should conduct "regulatory stress tests" on their data inventory. By categorising data into tiers (e.g., high-risk biometrics vs. low-risk behavioural patterns), companies can identify which assets are bargaining chips and which require immediate regional server infrastructure to ensure continuity.

6. Sector Specific Recommendations

These sector-specific guidelines reflect a realist adaptation to the distinct logics of sovereignty identified earlier, seeking to balance sector-specific risks with the realities of market access.

6.1. Automotive Industry

When regulating the automotive industry, states should prioritise protecting national and economic interests without stifling industry development. In this high-stakes environment, localisation is often a non-negotiable price of market entry; therefore, the goal is to refine its design

to prevent total isolation. Accordingly, states may require processing of sensitive personal data on the vehicle's edge computer rather than the cloud. This requirement reflects not only data protection concerns but also a counter-surveillance logic, as raw sensor and location data can reveal critical information about infrastructure usage, mobility patterns, and potential security vulnerabilities in real time.

Moreover, states can introduce tiered data classification for mapping, consisting of strategic infrastructure (such as HD maps) with strict locality requirements, operational data (such as battery health and tyre pressure) with allowed free flow, and, finally, safety-critical data with interoperability across brands locally. In this framework, HD maps are treated as dual-use assets: while they enhance driving accuracy and AI performance, they simultaneously provide high-resolution spatial intelligence that could be leveraged for military, intelligence, or large-scale surveillance purposes.

Ultimately, if a foreign manufacturer wants to use local driving data to train its global AI, states may allow it, provided that the shared information is anonymised and that "Anonymised Safety Insights" derived from it are transferred to local regulators to improve national road safety standards. This approach reframes data localisation not as pure restriction, but as a mechanism for transforming private data access into a public good, where knowledge extracted from data strengthens national safety infrastructures without exporting raw data.

On the other hand, companies should consider the unique characteristics of key markets and their specific data access frameworks. For instance, companies seeking entry into the Chinese market must be prepared to establish localised data infrastructure to comply with stringent national security and data sovereignty mandates. Moreover, during the localisation process, firms should proactively establish local data centres in key jurisdictions, utilise federated learning, and form partnerships for local mapping and sensor technology, as well as integrations with local insurance providers and municipal systems. Furthermore, a robust legal architecture must be established from the outset to determine data ownership, specifically whether the data belongs to the driver, the manufacturer, or the platform. Companies may also, from the outset, implement "geofenced" connectivity protocols, allowing a vehicle that crosses a border to switch its data-routing protocols to ensure all uploads stay within that specific jurisdiction's approved servers.

6.2. The Healthcare Industry

When regulating the healthcare industry, states should prioritise bio-sovereignty with research agility. Given the biopolitical sensitivity of health data, absolute data flow is often politically impossible; thus, policymakers should seek a 'second-best' equilibrium. Accordingly, states should implement tiered health data classification consisting of administrative health data with free flow, clinical data (patient history) with sovereign cloud and adequate

(Rabia Aydoğdu - Anadolu Agency)

protection requirements, and genomic data with strict localisation requirements. Genomic data, in particular, implicates long-term structural sovereignty, as it determines future research capacity, pharmaceutical innovation, and a state's bargaining power in global biotechnological markets.

Moreover, to avoid localisation costs, states should also create bilateral or multilateral "Research Corridors" with like-minded nations, enabling cross-border collaboration on rare diseases without compromising overall security. Such corridors are not designed to enable unrestricted data flows, but rather to allow limited, purpose-bound sovereignty concessions in pre-defined research contexts. This is important because, for example, multiple joint EU-U.S. health research initiatives have ended or been severely restricted due to the EU's GDPR.

Finally, to turn the local data pool into an investment in future national healthcare infrastructure, if a foreign AI firm trains a diagnostic model on a nation's public health data, the state should mandate that the resulting AI algorithm be provided to the national health service at a discounted price or as a "public good." In effect, this treats access to public health data as an implicit R&D subsidy, ensuring that the downstream value of data-driven innovation is partially re-internalised into the public healthcare system.

On the other hand, for companies, it is essential to focus on the unique characteristics of key markets and the increasingly stringent data sovereignty regimes in those markets. Accordingly, for example, companies entering the EU should adopt a 'sovereign cloud' approach to navigate the de facto localisation pressures of GDPR without halting cross-border research. In the Chinese healthcare market, firms must prioritise local data trusteeships to ensure that sensitive genomic and clinical data remain under domestic jurisdictional control. Moreover, instead of moving raw patient data to central headquarters, companies may establish federated learning or secure multi-party computation frameworks for AI training. In the healthcare context, these approaches increasingly represent not a second-best workaround, but an optimal governance-aligned solution that preserves both state control and corporate innovation incentives.

Partnering with local, state-backed entities to host health data, so that companies can satisfy regulators that the data is under local jurisdictional control, even if the underlying software belongs to the companies, could be another step for companies. Finally, companies may advocate for "patient-centric portability", which grants patients the power to consent out of localisation.

7. Conclusion

While data localisation is often framed as a privacy concern, it has evolved into a strategic geopolitical and economic tool used by states to assert digital sovereignty and foster domestic industrial growth. This shift is particularly evident in the high-stakes automotive and healthcare sectors, where the sensitivity of genomic, biometric, and geolocation data necessitates a transition from centralised global models to decentralised, interoperable frameworks. To navigate this fragmented landscape, states must balance national and economic security with innovation by adopting tiered regulatory regimes and prioritising technical interoperability. Concurrently, companies should move beyond mere compliance to embrace "localisation-by-design," utilising advanced technologies like federated learning and data trusteeships to transform data processing into a collaborative "bargaining chip" for market access. Ultimately, the future of global data governance depends on the ability of both private and public actors to align their interests, ensuring that data remains a shared driver of technological progress rather than a catalyst for permanent digital isolation.