TNO Vector

Sovereignty in the financial sector

Report on the European state of affairs

TNO Public ⟩ TNO 2025 R11291
16 June 2025

ICT, Strategy & Policy
tno.vector.nl
+31 88 866 00 00
info@tno.nl

TNO 2025 R11291 – 16 June 2025

Sovereignty in the financial sector

Report on the European state of affairs

Author(s)	Tom Barbereau
Report text	TNO Public
Number of pages	26 (excl. front and back cover)
Number of appendices	0
Project name	PMC Values based Digital Society
Project number	060.00460

Executive Summary

Europe's financial sector is at a pivotal juncture in its digital transformation journey. While national payment systems such as iDeal, Bizum, and Wero have proven that European-led fintech innovation can thrive, the broader digital infrastructure underpinning financial services and products remains heavily reliant on non-European providers. Hyperscalers (i.e., Microsoft, Amazon, Google) collectively hold most of Europe's cloud infrastructure market, with 92% of Western data stored in U.S.-owned infrastructure (Knafo 2025). In light of recent geo-political shifts, this dependency raises urgent concerns about strategic autonomy, sovereignty, and systemic risk.

This report frames the challenge as a trilemma between autonomy, control, and innovation - each representing a critical imperative for the financial sector. Navigating this triangle requires difficult trade-offs and strategic foresight. We explore relevant responses to provide straetgic guidance for decision-makers in the public and private sector.

AUTONOMY refers to the ability of institutions to make independent, long-term decisions without undue reliance on foreign infrastructure or policy environments. As digital infrastructure becomes more deeply embedded in financial operations, dependence on Big Tech undermines Europe's capacity to shape its own digital future. Strategic autonomy demands investment in domestic capabilities, access to alternative infrastructure, and the flexibility to evolve business models towards collaboration without being locked into proprietary ecosystems.

INNOVATION remains essential for competitiveness. Big Tech firms have redefined innovative capacities. Their platforms, which largely drove the FinTech movement, set new benchmarks for personalization, speed, and convenience - raising customer expectations across the board. For traditional financial institutions, keeping pace with this innovation is not optional. However, aligning too closely with Big Tech risks ceding control over data, differentiation, and trust - core assets in the financial sector over which we need to maintain a grip.

CONTROL encompasses the regulatory and institutional mechanisms that ensure financial stability, consumer protection, and resilient systems. As financial services become embedded in global digital ecosystems, traditional oversight frameworks struggle to keep pace. European regulation, including the Digital Operational Resilience Act (DORA), is beginning to address these gaps, but institutions must proactively manage partnerships and compliance in an increasingly complex environment.

This report explores the implications of this strategic trilemma and offers actions for European financial institutions to regain control without sacrificing innovation. It highlights the systemic risks of digital dependence, the emerging regulatory landscape, and the practical steps institutions can take to build resilience – such as diversifying providers, investing in sovereign cloud solutions, and strengthening internal governance.

The goal is not isolation, but strategic resilience: ensuring that Europe's financial infrastructure remains secure, competitive, and sovereign in a rapidly evolving digital landscape. For decision-makers such as CIOs, this means rethinking infrastructure strategy, aligning innovation with regulatory foresight, and championing digital sovereignty as a core pillar of institutional resilience.

Contents

1 Introduction

Increased concern amid geo-political tensions has alerted decision-makers to the European public sector's dependence on a small number of non-European technology providers. Crucially, as recently commented by Dutch parliamentarian Barbara Kathmann (see Vigliarolo 2025), author of four out of eight motions on sovereignty and strategic autonomy that passed parliament on 18 March 2025: *"with each IT service our government moves to American tech giants, we become dumber and weaker."*

This assertion holds for the private sector too. Dependence on foreign service providers – in particular digital technology providers – and the corresponding need to become resilient was recognized by TNO in sectors from health and mobility to manufacturing and mobility (Stolwijk et al. 2022). Just last year, in July 2024, the Microsoft outage triggered by an updated to 365 caused global chaos (Conger and Frenkel 2024). In the process, some of the largest European banks and financial institutions were hit.

For the European financial sector, and its increasingly digital modus operandi, this report enters into conversation with the 2024 year report of the Dutch Central Bank (2025) and highlights that sovereignty must be a topic of strategic importance.[1] In the context of this report, sovereignty shall manifest by reduced dependence (i.e. increased autonomy) from foreign digital service providers and Big Tech in particular.

While this report briefly touches upon sovereignty in payments infrastructures – as it is here that alternatives thrive because of regional needs, it thematizes the reliance of the financial sector on cloud services and the panoply of other products and services offered by Big Tech. As such, this report is intended for CIOs and senior technology leaders in the financial sector who are navigating the complexities of digital transformation, as well as government decision-makers who play a leading role in this context. It aims to support strategic decision-making by highlighting the tensions between innovation, control, and autonomy in an increasingly interconnected and externally dependent digital landscape.

1.1 Sovereignty in the European financial sector

The battle for sovereignty is well under way in one domain of finance: our payment infrastructures (Sandbu 2025). Much like utilities such as gas and water, payment systems are a vital part of the critical infrastructure that sustains our economy. However, they are still reliant on – predominantly American - providers such as Visa and Mastercard and more recently, technology providers such as Apple and Google (Bassens and Hendrikse 2022). Non-European payment networks and providers continue to be a key pillar in the value chain: The market share of Mastercard and Visa are estimated at 61% in Europe. In reflection to these numbers, the Dutch Central Bank (2025) asserts that it does *"not want our payment systems to be dependent on the policy of foreign governments,"* and that *"there must always be European options available, so that Europe can make its payments independently."*

[1] The topic of this report is not about sovereignty in the macro-economic, monetary sense. It does not address the role played by the euro, or the interdependence of financial markets. It also omits the topic of digital assets, stablecoins, and other types of virtual currencies.

Europe is fighting back on the payments front! While iDeal, launched 20 years ago and used daily by Dutch consumers, is often cited, national solutions like Swish in Sweden, Bizum in Spain, and Blik in Poland have also achieved remarkable success - often outperforming third-country providers in their home markets (for Sweden, see Sveriges Riksbank 2024; for Spain, see Martin 2024). Building on this momentum, Wero acts as a pan-European initiative striving to unify and expand these options. Each have their own limitations (see Cannataci et al. 2025).

These fairly successful developments in payments are not mirrored in the developments in the digital infrastructure for financial services. By contrast, as noted earlier this year in the European Parliament's draft report on technological sovereignty and digital infrastructure (Knafo 2025). It notes that "*the European cloud market is unquestionably dominated by US companies [as] Amazon Web Services, Microsoft Azure and Google Cloud hold approximately 69 % of cloud infrastructure market share in Europe,"* and that *"92 % of the West's data are stored in the USA, in infrastructure owned and operated by US providers."*

Encouraged by open banking regulations in the European Union, the financial sector has embraced and incorporated the services and products of foreign technology providers as the backbone of their operations (Barbereau, Weigl, and Pocher 2024). Amazon's AWS is now the go-to choice for the back end of gateways and payment processors – largely given its flexibility and depth in offering (Barbieri 2020). Close thereafter come Microsoft's Azure and GoogleCloud. Critically, Big Tech resorted to strategies that "*lock-in developers and customers [...] into a hybrid business model based on a synergy between hardware, software and data-driven platform components*" (Hendrikse, Bassens, and Meeteren 2018).

As data has become the driver of current business and future innovations in the financial sector (Xiong et al. 2016), with the help of Big Tech, the financial sector has become a business of platforms (banking as a service) where data is a core driver of innovation (Westermeier 2020; Ferrari 2022). In the process of that transformation and digital transition, whereby reliance on foreign service providers increased, the implications for strategic autonomy – for economic reasons and in terms of national security – are severe (Knafo 2025). Again, consider the Microsoft outage that caused global chaos and left the European financial sector in turmoil (Conger and Frenkel 2024).

Aside from the inherent, systemic risks posed by said reliance, the European Central Bank (2024) noted vulnerabilities related to data security, legal jurisdiction, and operational control. This aligns with the conclusion drawn by TNO (Stolwijk et al. 2024) that

> *"without digital sovereignty, there is the potential that [...] cyber-**attacks** can disrupt critical infrastructure, undermine national security, or even put citizen safety at risk."*

1.2 What next?

The globalized nature of the world, despite benefiting economic growth and innovation (Athreye and Cantwell 2007), is challenged by calls for strategic autonomy in response to the increased reliance on foreign service providers and associated risks. Though the conversation around that autonomy started with the call for privacy, it is about our – as Europeans – control over the use *and* development of digital infrastructures, data, and technology.

Becoming more autonomous comes at a cost. The affordances of technological and digital infrastructures provided by Big Tech allowed European financial institutions to innovate and be ready for a generation of users native to the Internet. The strategic coupling between finance and technology was necessary to stay competitive (Hendrikse, van Meeteren, and Bassens 2020).

The question is **how can European financial institutions maintain control while staying competitive and innovative?** Can we escape the vendor lock-in we subjected ourselves to? How to deal with the consequences of our possible dependence? Where to start and what does it take to gain independence?

Because we observe domestic solutions outperforming Big Tech on the level of payments, we do not engage with this discussion in greater detail. Instead, the focus here is on the reliance of Big Tech's digital infrastructure by the financial sector.

1.3 Reading guide

The report is structured as follows: Section 2 introduces the current landscape, including relevant deep dives into the consequences of our dependence. we here present the trilemma for the financial sector. Section 3 presents European responses to the dependence and introduce alternatives. We here highlight practical steps for the financial sector to deal with the trilemma. Section 4 provides an outlook.

2 The trilemma faced by the European financial sector

2.1 A brief history of digitisation in the financial sector

The financial sector underwent a profound transformation driven by the rise of the Internet and more generally, the use of digital technologies in open banking. The COVID-19 pandemic has accelerated this digital transformation, leading to more diverse, competitive, efficient, and inclusive financial services in many economies (Goodell 2020). Prior to the discussion of open banking, the rise of FinTech and entrance of Big tech, let us take a step back and look at the reforms that emerged in response to the financial crisis of 2007-2008.

2.1.1 Reforms to the financial sector

The global financial crisis exposed fundamental weaknesses in financial regulation and supervision across Europe (Hodson and Quaglia 2009). In its aftermath, European policymakers launched a far-reaching overhaul of the financial rulebook aimed at restoring stability, rebuilding trust, and preventing future systemic failures. The pre-crisis model – largely based on national supervision and light-touch regulation ('rules on the book') – gave way to a far more integrated, supervisory and enforcement based framework at the EU level ('rules in action') (Moloney 2010).

The set of reforms on Capital Requirements (CR Directives I-IV) and the Capital Requirements Regulation (CRR), which came into force between 2009 and 2014, implemented the Basel III standards [2] in Europe and significantly increased capital and liquidity requirements for banks. To improve transparency and market discipline, the Markets in Financial Instruments Directive II (MiFID II) and its accompanying regulation (MiFIR), which took effect in 2018, expanded oversight of trading activities and enhanced investor protections. The European Market Infrastructure Regulation (EMIR), which entered into force in 2012, targeted systemic risk in derivatives markets by mandating central clearing and trade reporting.

While motivated by the crisis, these reforms were not just about correcting the past – they also aimed to prepare the sector for a rapidly evolving future. Even as new rules were being implemented, the financial industry was undergoing a parallel transformation driven by digitalisation. Technologies such as cloud computing, mobile banking, and real-time data analytics were beginning to redefine how financial services operated and were consumed. Indeed, while these reforms were hugely important, they largely responded to the previous crisis and did not fully anticipate the new kinds of risks emerging from this technological shift. Digital technologies were primarily viewed as opportunities for innovation, efficiency, and expanded access, rather than as potential sources of systemic risk. This optimism

[2] Basel III refers to an internationally agreed set of measures formulated by the Basel Committee on Banking Supervision in response to the financial crisis. These aim to strengthen the regulation, supervision, as well as risk management of banks.

helped pave the way for developments like open banking and the rapid rise of FinTech – bringing both new possibilities and unforeseen regulatory challenges.

2.1.2 Open banking and FinTech

In the mid 2010s, the shift to open banking – the idea of providing third-party developers access to data from traditional banking systems through APIs (Zachariadis and Ozcan 2016) – empowered new entrants to challenge traditional financial institutions by offering innovative solutions (Stefanelli and Manta 2023). Leveraging big data, artificial intelligence, and other emerging technologies, these players have disrupted the modus operandi: fostering data-driven personalisation, faster (and cheaper) transactions, and broader access to underserved populations. FinTech is a game-changing challenger; data is the prize everyone's chasing (Ferrari 2022; Bassens and Hendrikse 2022; Westermeier 2020).

The traditional financial sector has responded to the advent of open banking and the rise of these FinTechs with a mix of adaptation and collaboration through partnerships (Feyen et al. 2021). Initially, many traditional banks viewed FinTech as a disruptive threat, but over time, they recognized the potential for synergy. Banks have increasingly embraced digital transformation, investing in digital technologies to enhance their operations, expand services and improve customer experience. They have also created or formed strategic partnerships with companies to leverage their innovative solutions, such as advanced data analytics and personalized financial services. This collaborative approach has allowed traditional banks to remain competitive, foster innovation, and meet the evolving demands of their customers (Barakova, Ehrentraud, and Leposke 2024).

European regulators too had to account for these dynamics. In the mid-2010s, they began to lay groundwork for a regulatory approach that would later expand. The Revised Payment Services Directive (PSD2), adopted in 2015 aimed to foster innovation and competition by mandating banks to open their payment infrastructure and customer data (with consent) to third-party providers, effectively laying the foundation for open banking. At the same time, the General Data Protection Regulation (GDPR), enforced from 2018 onwards, established strict rules around data privacy and protection, directly affecting how financial institutions collect, process, and share personal information.

2.1.3 Big Tech is here (to stay?)

As part of the open banking and FinTech wave, digital service, and product providers – commonly known as Big Tech firms – played a major role in accelerating digital transformation and disrupting financial markets. They benefited significantly from economies of scale and capitalized on the network effects inherent to open banking (Bassens and Hendrikse 2022). Crucially, these firms were non-European.

To do so, they used a number of strategies:[3]

- Offering of technology services: Big Tech firms have a panoply of offering that is attractive to the financial sector. While FinTech unicorns Revolut and Bunq rely on GoogleCloud and AWS respectively; incumbent financial institutions to rely on these firms to innovate and remain competitive – from access to cloud-scale analytics to artificial intelligence. To meet its business needs, DZ Bank migrated from on-premises

[3] The list of strategies is non-exhaustive. What are disclosed here are some of the key strategies used by Big Tech's venture into the financial sector with a particular focus on Europe.

virtual machines to GoogleCloud; the Danske Bank migrated its servers to AWS; and Rabobank relies on Azure and Power BI. There are countless other examples.[4]

- Entering into partnerships: Big Tech firms like Apple and Google have partnered with established financial institutions like Goldman Sachs (Apple Card) and GooglePay (with various banks) to enter the world of payments. Typically, such partnerships allows to navigate regulatory complexities in the financial sector while leveraging the expertise of incumbents (Barakova, Ehrentraud, and Leposke 2024).
- Focusing on payment solutions as anchor: Big Tech firms have used payment solutions as an entry point to embed themselves within financial ecosystems (Canepa 2022). Services like Amazon Pay, Apple Pay, and Google Pay serve not only as consumer-facing tools but also as gateways to (back-end) technological services - such as cloud infrastructures, analytics, and APIs - to merchants and financial institutions.
- Focusing on credit services as anchor: Amazon, Alibaba and others have ventured into lending services, providing loans to merchants on their own platforms based on credit assessments of (different) data than incumbents. This strategy helps them support their ecosystem while generating additional revenue streams (Cornelli et al. 2020).
- Deploying disruptive technologies: Big Tech firms have explored alternative digital technologies. For example, Meta's attempt to launch Libra (now Diem) aimed to create a global digital crypto-currency, though it faced significant hurdles and was eventually shut down by US regulators. We are likely to see more of these experiments (Kaniadakis and Foster 2024).

The inherent ability to scale digital platforms, encourage Big Tech to deepen their involvement in the provision of financial services and products. From the FactSet Supply Chain Relationships database,[5] we conclude that the strategies followed resulted in deep ties between Big Tech Firms and European banks (TABLE 2.1). A more substantive assessment of these dependencies is expected to deliver additional conclusions (Knafo 2025).

[4] Each of these are extracted from respective pages from AWS Case Studies: Financial Sector (link), Microsoft Customer Stories (link), and Google Cloud Customer Stories (link).

[5] The database includes supplier-customer relationships and associated keywords. It has previously been used by TNO and the Joint Research Center to map supply chains. Here, Big Tech firms were matched with EU banks. That is, companies whose headquarters are in a EU27 member state and that are classified by FactSet as belonging to one of the following industries: 'major banks', 'regional banks', 'savings banks', and 'investment banks/brokers.' Note that the company relationships mapping by FactSet is non-exhaustive.

Provider	Product/service	European financial institution
Alphabet	Google Cloud, Google Workspace (G Suite), Google Data Studio (Looker Studio), Google Maps Platform	Deutsche Bank (DE), Commerzbank (DE), Deutsche Börse (DE), ABN AMRO Bank (NL), Banco Bilbao Vizcaya Argentaria (ES), BPER Banca (IT)
Microsoft	Windows Phone Platform (Mobile Banking), Platform Software, Windows, Microsoft Dynamics 365, cloud (Azure), Microsoft BizTalk (server)	Privredna Banka Zagreb (HR), Diebold Nixdorf (DE), Rabobank (NL), Saxo Bank (DK), Banco Popular Espanol (ES)
Amazon	e-commerce partnership, cloud (AWS)	Crédit Agricole (FR), Banco Bilbao Vizcaya Argentaria (ES)

TABLE 2.1 Overview of supplier-customer relationships between US Big Tech providers and EU financial institutions identified by FactSet.[6] The location country of the banks is indicated in parentheses. Data source: FactSet Supply Chain Relationships (reference date: 24-5-2025).

2.2 The world has changed

Most recently the world has changed once again with technology, including digital technology infrastructure for the financial sector, becoming a crucial factor or instrument of geopolitical nature. For example. in response to the Russian invasion of Ukraine, global sanctions to the financial sector were put in place. In its first package of sanctions of February 2022, the Union limited the "*ability of the Russian state and government to access the EU's capital and financial markets and services.*" Mastercard, PayPal, Apple, and other corporations followed suit soon after.

Most recently, in an escalating transatlantic trade war, Big Tech and its regulation in Europe is used as a bargaining chip (Rankin 2025). The Trump administration is actively pushing back on rules made in Europe. Now more than ever it is time to consider the consequences of on the strong dependence of Big Tech and the geopolitical tension. As for other sectors: what happens if Microsoft is compelled to flick the switch on Europe? What if Amazon does? Aside from the geopolitical tensions, it may also be time to question the impact of the European rules. Are they enough? Are they effective? And, in reflection on Mario Draghi's (2024) conclusions, how are the rules impacting innovative capacity?

Beyond such extreme but necessary thought exercises (Ness 2025), the financial sector's dependence on third-country providers and Big Tech introduces several risks that request careful consideration. A non-exclusive list of such risks is presented in TABLE 2.2 Subsequently, we deep-dive into three of these risks.

[6] Note that this overview includes both historical and ongoing relationships and that no relationships were identified for Meta (Facebook) or Apple.

Risk Type	Description	Implications
Systemic & Operational	Heavy reliance on a small number of non-EU providers for critical infrastructure, products, and services.	Creates lock-ins and single points of failure; limited control over continuity, security, and compliance; heightened macroprudential risk.
Market & Strategic	Big Tech's entry into finance with unmatched data capabilities and proprietary ecosystems.	Distorts competition and innovative capacity; undermines EU financial autonomy; limits ability to pivot or support local innovation.
Regulatory & Values-Based	Misalignment with EU regulations and norms; external control over sensitive data.	Difficult supervision over data aggregation and usage; risks to GDPR, DORA, and digital sovereignty; potential erosion of core European values.

TABLE 2.2 Overview of risks.

2.2.1 (Vendor) lock-ins and points of failure as systemic risks

Out of the non-exclusive list of risks, we highlight the risk posed by lock-ins. The risk of lock-in arises when financial institutions become deeply embedded within proprietary ecosystems – such as one-stop-shop cloud platforms and application programming interfaces (APIs). The dependence is highlighted in TABLE 2.1.

While these systems offer powerful capabilities and operational efficiencies, they often come with high switching costs, limited interoperability, and contractual restrictions that constrain future flexibility (Hendrikse, Bassens, and Meeteren 2018). Over time, this dependency can undermine a firm's ability to adapt its digital strategy, negotiate favourable terms, or align with evolving regulatory needs or other strategic goals. Lock-in is not just a technical or vendor issue – it is a strategic vulnerability that can limit innovation, compromise autonomy, and expose institutions to external decision-making beyond their control (Prudential Regulation Authority 2023).

From a systemic perspective, lock-ins are a form of dependence that creates single points of failure at the level of third parties. Rightfully, Denis Beau (2018), First Deputy Governor of the Bank of France, warned that "*as the core financial functions lift and shift to the cloud, the risk of a single point of failure will emerge.*" The ripple effects caused by Microsoft's outage in 2024 are a case in point. Other examples that highlight such single points of failure – for the financial sector – are in cybersecurity. Beau further argues that

> *"with greater interconnections between [digital] technologies and the financial system, cyber-risk is moving from an idiosyncratic risk to a potential source of systemic risk."*

Crucially, the Digital Operational Resilience Act (DORA) that is applicable since 2025, aims to strengthen the resilience of the financial sector against ICT-related disruptions will shift responsibility such that financial institutions that outsource technology services are ultimately responsible for risk management. This does not mean they carry responsibility alone: DORA also establishes that the European Supervisory Authority is to appoint observers for each critical third-party service provider (i.e., Amazon, Microsoft, etc.), to assess their mechanisms for managing the risks posed to financial institutions.

2.2.2 Entrenchment and innovation drag as market risk

From an economic perspective and view on innovation systems, the described dominance of few foreign firms can – in the long run - have negative effects on the competitive dynamics of the financial sector (de la Mano and Padilla 2018). When institutions become dependent on a small number of providers, they lose bargaining power, face high switching costs, and often must conform to proprietary technologies or data formats. This dependence, while accelerating the spread of innovations (Stolwijk et al. 2022), can stifle the adoption of alternatives – here, the emerging European innovators or regional solutions – which may struggle to integrate or meet compatibility requirements with entrenched ecosystems. On the other hand, these very innovators are dependent on the digital technology providers described throughout this article. Over time, this dynamic creates barriers to entry, narrows the pool of viable suppliers, and erodes market diversity.

The long-term consequence is a drag on innovation; that is, because new entrants are the ones typically driving innovation (OECD 2020). When a handful of firms set the pace and standards for digital capabilities, the sector may be locked into innovation cycles and product roadmaps over which they have little influence. Smaller firms and startups – particularly those rooted in Europe - find it harder to compete, not because of inferior offerings, but because the path to scale is blocked by closed architectures and entrenched customer dependencies (Brits et al. 2021). Furthermore, and given the present geo-political climate, it may be strategically desirable to be as independent as possible from the start.

As a result, innovation becomes incremental and centrally controlled, rather than diverse, responsive, and competitive. Without open alternatives and interoperable standards, the broader ecosystem risks becoming less dynamic, less inclusive, and ultimately less resilient (Mohn and Barbereau 2025).

2.2.3 Legal vulnerability and data protection

For European financial institutions that rely on an American cloud service provider, the U.S. CLOUD Act presents notable legal and operational implications. The Act, which came into force in March 2018, empowers U.S. law enforcement authorities – under certain conditions and with appropriate court orders – to compel access to electronic data held by U.S.-based companies, regardless of where the data is physically stored. This means that a European firm storing customer data with a U.S. cloud provider may find that such data could be subject to lawful access requests by U.S. authorities if deemed relevant to a criminal investigation (Rojszczak 2020). This can create a potential conflict between compliance with EU data protection regulations – particularly the GDPR – and the extraterritorial reach of U.S. law.

Given the sensitivity of the financial sector and the critical need to ensure data confidentiality, integrity, and sovereignty, European financial institutions must pay particular attention to the implications of the CLOUD Act. Even if the cloud infrastructure used is physically located in Europe, the fact that the service provider is a U.S.-based company or has corporate ties is sufficient to bring the data within the potential reach of U.S. authorities

(Blancato 2024). Additionally, contractual or operational arrangements where joint controllers or processors have affiliations with U.S. firms can also expose the data to U.S. jurisdiction under the Act. For institutions managing confidential financial and personal data, this scenario raises significant concerns over data privacy and the possible erosion of trust.

Less apparent risks also exist. For example, if the European financial institution tailors services to U.S. clients – whether intentionally through targeted marketing or unintentionally by serving U.S.-based customers – this can deepen the institution's exposure to the CLOUD Act.[7] Revenue generation from U.S. clients or even behavioural insights obtained from their interactions can be viewed as creating a sufficient nexus with the U.S. to attract legal interest. Conversely, avoiding direct targeting or engaging only passively with U.S. customers may reduce exposure, although it does not eliminate all legal uncertainty.

2.3 Trilemma of strategic autonomy

The points made until now point to the heart of the discussion on sovereignty. There is complexity to the financial sector; one that is more stylized in terms of a three-cornered trilemma (FIGURE 2.1) consisting of autonomy, control, and innovation. Between each of these corners lie respective imperatives.

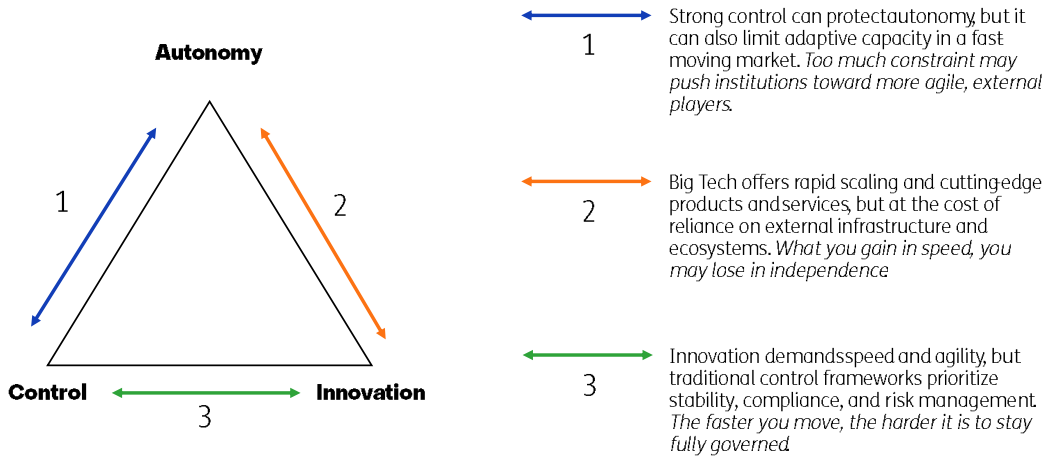

FIGURE 2.1. Strategic trilemma and its imperatives for the financial sector.

2.3.1 Autonomy

Strategic autonomy refers to the capacity of a system – or institution – to make independent, long-term decisions in the face of external pressures or dependencies (Stolwijk et al. 2024). In a digital world dominated by Big Tech firms, financial institutions risk becoming reliant on infrastructure they do not control, and beholden to data ecosystems they do not govern (Bassens and Hendrikse 2022). In the face of the systemic and market risks discussed, this undermines our ability to shape our own digital futures and erodes trust.

For both public and private sector leaders, remaining sovereign and preserving strategic autonomy means investing in domestic capabilities (i.e., having access to alternatives), ensuring access to critical infrastructure, and retaining the flexibility to adapt business models without overexposure to lock-in's or at the expense of innovative capacity.

[7] See also: Newsletter #96 (from 30 Sep 2022) | European Data Protection Supervisor.

2.3.2 Innovation

As argued, Big Tech firms are redefining what financial services look like or, as Denis Beau (2018) writes "*FinTech's are the talk of the town but Big Techs are the real deal [because they have] the potential to fundamentally redefine financial intermediation beyond the universal banking model toward integrating financial services within a universal ecosystem.*" With artificial intelligence, real-time data analytics, and globally scaled platforms, they deliver seamless experiences – from frictionless payments and cloud-enabled analytics to instant credit decisions and agile platforms. These firms set new benchmarks for efficiency, personalisation, and convenience, raising customer expectations across the board. For traditional financial institutions, aligning with this pace of innovation is no longer optional – it's a matter of survival (Doerr et al. 2023).

However, as banks lean into tech partnerships or adopt Big Tech infrastructure to remain innovative, they risk ceding critical elements of data ownership, relevance, and potential distinction in terms of trust. Regulation proposed and adopted in Europe is only now providing the necessary frame to strike this balance in a responsible manner.

2.3.3 Control

Control represents the regulatory and institutional need to safeguard financial stability, protect consumers, and manage risk. Traditional financial institutions operate under strict oversight frameworks – capital requirements, anti-money laundering / know-your-customer regimes, stress testing, etc. – which ensure accountability and resilience. Yet, as financial services become embedded within digital ecosystems that operate across jurisdictions and often outside the perimeter of banking regulation, traditional control mechanisms can become fragmented or obsolete (Bassens and Hendrikse 2022; Barbereau, Weigl, and Pocher 2024). In parts, European legislation is now ensuring that responsibility where it ought to be.

For organisations, the challenge is how to maintain robust governance and compliance while integrating – or competing with – entities that do not per se play by the same rules. This requires controlling the partnerships more accurately – something financial institutions will now be compelled to under DORA.

3 Responses

3.1 European responses and alternatives

3.1.1 Regulatory responses

The European regulatory response to the growing trilemma between innovation, control, and strategic autonomy – particularly in the face of Big Tech's expanding role in financial infrastructure – has been increasingly assertive. A cornerstone of this response is DORA, which applies since early 2025. DORA marks a significant step toward harmonizing risk management across the EU financial sector and explicitly brings critical third-party providers, including major cloud and software vendors, under the supervisory umbrella of European authorities (Kun 2024). It introduces mandatory risk management frameworks, advanced resilience testing (e.g., threat-led penetration testing), and real-time incident reporting – all designed to ensure financial institutions remain operationally resilient in the face of digital disruptions.

Meanwhile, the revised Payment Services Directive (PSD2) which came into effect in 2019 lays the groundwork for secure and trusted data sharing mechanisms around payment data. It does by clarifying the liability regime, enhancing consumer protection, prohibiting surcharges by payment service providers, and increasing the security for payment services via customer authentication.

Aside from other legislations (incl. for example, on crypto-assets), these are expected to have an overall positive impact on the financial sector as each reflects a shift in the EU's regulatory posture – from reactive compliance to proactive shaping of digital ecosystems (Barbereau, Weigl, and Pocher 2024). For financial institutions, this means aligning innovation strategies with this legislative arc. While at a potentially greater cost in the short term, in the long term the aim should be to minimize exposure to non-EU dependencies, building operational resilience, and contributing to a more sovereign and secure European financial landscape.

3.1.2 Existing alternatives

There are several initiatives that represent significant strides in creating alternatives to traditional financial and data infrastructure. On the level of payments, as mentioned before, numerous alternatives exist. Account-to-account payment networks like iDeal, Swish, Bizum, and Wero are designed to compete with the likes of PayPal. Each foster European strategic autonomy for a significant part of the payment value chain. However, aside from the ambition of Wero, none of these are truly pan-European, silver bullet solutions. Academics flagged significant hurdles to its success (Judt and Krueger 2021).

On the level of infrastructures there are pan-European initiatives. Gaia-X aims to establish a federated data infrastructure, promoting data sovereignty and collaboration among European entities (Blancato 2024). The European Blockchain Services Infrastructure (EBSI) seeks to leverage blockchain technology for cross-border services, enhancing transparency and efficiency in transactions. Both could provide viable alternatives to specific players in the value chain. Each, however, do not provide the full solution at the moment: Gaia-X is active

in developing technical standards (Goujard and Cerulus 2021), EBSI has few concrete applications (Munster 2024).

3.1.3 Emerging alternatives

Another core, pan-European alternative – even though caught up in political debates (Faggionato and Munster 2024) – would be the digital euro. It is an effort by the European Central Bank (ECB) to introduce a European payments network, challenging the status quo, which is dependent on the duopoly of Visa-Mastercard and dollar-backed digital currencies (stablecoins). It was argued that the digital euro is "*driven by European security rationales and [contributes] to the agenda of resilience and autonomy*"(Westermeier 2024). Indeed, according to the ECB's Piero Cipollone (2025), the digital euro is "*the moment to make Europe's strategic autonomy in the critical area of payments a reality*." However, it remains to be seen to what extent the digital euro will address privacy concerns (Cannataci et al. 2025) and curb respective agenda of regional independence on the level of Member States (Brunnermeier and Landau 2022).

At last come ambitious grass-root led initiatives. In 2024, the Eurostack was proposed (see Bria, Timmers, and Gernone 2025). To date the Eurostack is a policy vision that aims to build and develop "*a complete digital ecosystem made and supplied in Europe*." The ambition has received traction at the level of the Commission and individual Member States, as well as industry representatives (Toffaletti 2025). It remains to be seen to what extent such initiatives will find applicability in the financial sector. To date, the Eurostack's price tag is estimated at 300 billion euros (Bria, Timmers, and Gernone 2025). In the same year, another such initiative is the policy roadmap of Reclaiming Digital Sovereignty that proposed a "*progressive reform agenda to enhance digital sovereignty for people and the planet*" (see Rikap et al. 2024).

3.1.4 Lessons learned

Attempts to build sovereign European infrastructure – although often relative recently started and therefore difficult to evaluate in terms of success – stumble in various cases due to a mix of misaligned incentives, slow execution, and fragmented governance. Simply declaring the need for "sovereignty" is not enough (Glasze et al. 2023). Success requires clear value propositions for private actors, technical competitiveness of global alternatives, and fast, modular execution and adaptability – all of which are essential to scale solutions (Gil-Garcia and Flores-Zúñiga 2020). In various cases, public-private initiatives struggle because they are too top-down, too slow to deliver early value, or too constrained by political compromise across diverse member states (Anthopoulos et al. 2016).

Another key lesson is that sovereignty cannot be achieved through protectionism (Glasze et al. 2023) – solutions must be competitive on merit, and should focus on usability, and integration. Failure to attract meaningful adoption often stems from a lack of product-market fit, unclear governance models, or failure to prioritize user experience and developer ecosystems. Finally, overly rigid, or abstract definitions of sovereignty and strategic autonomy can alienate partners. A more pragmatic, layered approach – focusing on strategic autonomy in key areas (data, identity, infrastructure) (Stolwijk et al. 2024) and control points in value chains (Pisa et al. 2024) – are needed to gain more traction.

3.2 Actions to solve the trilemma

Solving the tension between innovation, control, and strategic autonomy requires a shift from binary thinking to intentional balancing. Rather than choosing between agility and accountability, or between global platforms and local independence, financial institutions must pursue a hybrid digital strategy – one that ensures competitive and innovative capabilities while reducing structural dependencies over time; one that includes several measures and solutions.

3.2.1 Cost and benefits of autonomy

Stakeholders must first evaluate the cost-benefit trade-offs of technological dependency (or, on the other side of that coin, the cost-benefit of technological autonomy). Leveraging foreign networks or Big Tech infrastructure may accelerate innovation in the short term, but what are the long-term costs in terms of vendor lock-in, compliance blind spots, and reduced strategic flexibility?

Conversely, achieving strategic autonomy – by investing in sovereign infrastructure, open standards, and internal capabilities – may carry upfront costs, but builds long-term resilience and optionality. Evaluating each of these costs will greatly enhance decision making capabilities and agenda setting at the level of organisations.

The starting point to do so is an assessment of the status quo. An example of this was provided by the Municipality of Amsterdam in March 2025 (van Trigt 2025). Notably, together with the Technical University Delft and the AMS Institute, it developed a decision tool to help municipalities incorporate strategic autonomy into their digital procurement processes.

3.2.2 Technological alternatives as viable substitutes

Europe is actively fostering alternatives, from cloud and data initiatives (such as those led by the European Union) to payments infrastructures (such as the digital euro) and networks (such as Wero). Stakeholders should systematically evaluate and test existing and emerging solutions, using regulatory sandbox environments, pilot programs, and research projects to understand scalability, security, and integration potential. This allows leaders to make informed decisions on when and where these alternatives offer viable substitutes – or complementary layers, as choice in the 'worst case scenario' (Pisa et al. 2024) – to global offerings.

TNO has made the case for the development of a technology-driven paradigm of strategic autonomy (Stolwijk et al. 2024). This could include the creation (or contribution to) distributed cloud or cloud agnostic solutions, as well as artificial intelligence developments that meet public interests (see Barbereau and Dom 2024 for GTP-NL); the development of EU-based automated compliance tools; and, the integration functionalities beyond identification and authentication as part of the European digital wallet. The digital euro too presents a viable opportunity for research as questions of adoption and integration by commercial banks remain fuzzy.

An alternative strategy is the move towards open source software. In June 2025, the Danish government announced it will start moving away from Microsoft Office to LibreOffice (Vaughan-Nichols 2025). Financed by the German government since 2024, the openDesk suite too presents a viable open source alternative. openDesk combines other open tools like Nextcloud and Open-Xchange (Kindermann 2024).

3.2.3 Value chains and control points

The pragmatic approach to the present dependence in digital value chains is to develop a hybrid strategy with a focus on control points. Control points, following TNO (Pisa et al. 2024), are about

> *"securing resources that provide a competitive advantage and are of economic importance to a specific company."*

Here, the resource are information technology and data as assets that are part of a specific value chain (see Brynjolfsson 1994). Doing so starts by mapping critical functions through the technology stack and assess at which points the reliance on foreign providers is most critical.[8] Then, diversify by integrating trusted European or sovereign-aligned components as alternatives. It is imperative to build optionality into the technology stack to remain flexible as new alternatives mature and standards emerge; all while not treating the layers in isolation given that they influence each other.

Physical infrastructure remains and is a core component of digital value chains (see also, Blancato 2024). Notably, it is one of the drivers behind the European Union's AI Continent Action Plan. Here, and well beyond artificial intelligence, the cooperation and investments by private sector organisations to take initiatives off the ground is pivotal. The questions remain where to start? Where lies the greatest urgency? What are the costs? These are questions that all need to be considered in the analysis of value chains and are part of getting a grip on control points.

3.2.4 Collaboration

Stakeholders must actively engage with public, public-private and private led initiatives shaping the digital finance ecosystem with a specific agenda of sovereignty. This means participating in standardisation bodies, contributing to policy consultations, and – most importantly – driving and investing in existing or emerging digital infrastructure projects as alternatives. This requires collaboration.

Indeed, strategic autonomy is not built in isolation – it's built through collaborative, forward-looking ecosystems. Taking such approach means recognizing that no single actor – whether a state, company, or institution – can independently secure the capabilities, resilience, and innovation required to thrive in a complex, interconnected world (Mohn and Barbereau 2025).

[8] Criticality can come in different flavors. It may be about cost points, risk exposure, or other factors.

4 Outlook

For the European financial sector, the question of digital sovereignty is no longer theoretical – it is urgent. As European alternatives to Big Tech infrastructure begin to mature, institutions must act now to avoid future dependency risks. Waiting until alternatives are fully developed risks locking in architectures, data flows, and vendor relationships even further. Being proactive today means optionality tomorrow.

To maintain control while continuing to drive innovation, European financial institutions need a clear and deliberate roadmap. This includes short-term steps like diversifying digital technology procurement, exploring local infrastructure partnerships, and contributing to pan-European initiatives. Longer term, it means aligning digital strategy with public policy goals, investing in sovereign-capable technological alternatives, and shaping the regulatory frameworks that will govern tomorrow's financial ecosystem. Strategic autonomy is a moving target – those who build toward it early will define its future.

Acknowledgements

Thanks to Arnoud van Bree for his contribution to TABLE 2.1. I also thank the following experts for their contributions to this publication: Alexander van den Wall Bake, Claire Stolwijk, Augustinus Mohn, Olga Batura.

References

Anthopoulos, Leonidas, Christopher G. Reddick, Irene Giannakidou, and Nikolaos Mavridis. 2016. "Why E-Government Projects Fail? An Analysis of the Healthcare.Gov Website." *Government Information Quarterly* 33 (1): 161–73. https://doi.org/10.1016/j.giq.2015.07.003.

Athreye, Suma, and John Cantwell. 2007. "Creating Competition?: Globalisation and the Emergence of New Technology Producers." *Research Policy* 36 (2): 209–26. https://doi.org/10.1016/j.respol.2006.11.002.

Barakova, Irina, Johannes Ehrentraud, and Lindsey Leposke. 2024. "A Two-Sided Affair: Banks and Tech Firms in Banking." *Bank of International Settlements FSI Insights* 60 (October). https://www.bis.org/fsi/publ/insights60.pdf.

Barbereau, Tom, and Lieke Dom. 2024. "GPT-NL: Towards a Public Interest Large Language Model." In *2nd Workshop on 'Public Interest AI.'* https://publications.tno.nl/publication/34643373/5aTCTsaH/barbereau-2023-gpt.pdf.

Barbereau, Tom, Linda Weigl, and Nadia Pocher. 2024. "Financial Regulation, Political Context, and Technology in the European Union." In *Decentralization Technologies: Financial Sector in Change*, edited by Gilbert Fridgen, Tobias Guggenberger, Johannes Sedlmeir, and Nils Urbach, 19–46. https://doi.org/10.1007/978-3-031-66047-4_2.

Barbieri, Vittoria. 2020. "The Use of Cloud Computing by Financial Institutions." Cloud Banking Forum. European Banking Federation. https://www.ebf.eu/wp-content/uploads/2020/06/EBF-Cloud-Banking-Forum_The-use-of-cloud-computing-by-financial-institutions.pdf.

Bassens, David, and Reijer Hendrikse. 2022. "Asserting Europe's Technological Sovereignty amid American Platform Finance: Countering Financial Sector Dependence on Big Tech?" *Political Geography* 97 (August):102648. https://doi.org/10.1016/j.polgeo.2022.102648.

Beau, Denis. 2018. "Digital Finance, Market Disruption, and Financial Stability." *Bank of International Settlements Central Bankers' Speeches*, November. https://www.bis.org/review/r181113b.htm.

Blancato, Filippo Gualtiero. 2024. "The Cloud Sovereignty Nexus: How the European Union Seeks to Reverse Strategic Dependencies in Its Digital Ecosystem." *Policy & Internet* 16 (1): 12–32. https://doi.org/10.1002/poi3.358.

Bria, Francesca, Paul Timmers, and Fausto Gernone. 2025. "EuroStack – A European Alternative for Digital Sovereignty." Bertelsmann Stiftung. https://www.euro-stack.info/docs/EuroStack_2025.pdf.

Brits, Hans, Ge Cuijpers, Nicole Jonker, Melanie Lohuis, Ria Roerink, Coen ter Wal, and Annelotte Zwemstra. 2021. "Changing landscape, changing supervision: Developments in the relationship between BigTechs and financial institutions." Jaarverslag. De Nederlansche Bank (Dutch National Bank). https://www.dnb.nl/media/32apiuom/dnb-big-tech-supervision-changing-landscape-changing-supervision.pdf.

Brunnermeier, Markus, and Jean-Pierre Landau. 2022. "The Digital Euro: Policy Implications and Perspectives." *European Parliamentary Research Service*, January. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703337/IPOL_STU(2022)703337_EN.pdf.

Brynjolfsson, Erik. 1994. "Information Assets, Technology and Organization." *Management Science* 40 (12): 1645–62. https://doi.org/10.1287/mnsc.40.12.1645.

Canepa, Allegra. 2022. “The Role of Payment Services in the Development of the Big Tech Ecosystem.” *European Business Law Review* 33 (7). https://doi.org/10.54648/eulr2022043.

Cannataci, Joe, Benjamin Fehrensen, Bernd Lucke, and Mikolai Gütschow. 2025. “Digital Euro: Frequently Asked Questions Revisited.” University of Hamburg. https://www.wiso.uni-hamburg.de/fachbereich-vwl/professuren/lucke/bilder/digital-euro-faqs-revisited-10-1-25.pdf.

Cipollone, Piero. 2025. “Empowering Europe: Boosting Strategic Autonomy through the Digital Euro.” *European Central Bank Speech*, April. https://www.ecb.europa.eu//press/key/date/2025/html/ecb.sp250408~40820747ef.en.html.

Conger, Adam, and Sheera Frenkel. 2024. “Chaos and Confusion: Tech Outage Causes Disruptions Worldwide.” *The New York Times*, July 19, 2024, sec. Business. https://www.nytimes.com/2024/07/19/business/microsoft-outage-cause-azure-crowdstrike.html.

Cornelli, Giulio, Jon Frost, Leonardo Gambacorta, Raghavendra Rau, Robert Wardrop, and Tania Ziegler. 2020. “Fintech and Big Tech Credit: A New Database.” *Bank of International Settlements Working Papers* 887 (September). https://www.bis.org/publ/work887.htm.

De Nederlansche Bank. 2025. “DNG Jaarverslag 2024: Robuust beleid in een onzekere wereld.” Jaarverslag. De Nederlansche Bank (Dutch National Bank). https://www.dnb.nl/media/mtyf3rtu/dnb-jaarverslag-2024.pdf.

Doerr, Sebastian, Jon Frost, Leonardo Gambacorta, and Vatsala Shreeti. 2023. “Big Techs in Finance.” *Bank of International Settlements Working Papers* 1129 (October). https://www.bis.org/publ/work1129.pdf.

Draghi, Mario. 2024. “The Future of European Competitiveness: A Competitiveness Strategy for Europe.” European Commission. https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en.

European Central Bank. 2024. “ECB Guide on Outsourcing Cloud Services to Cloud Service Providers.” *European Central Bank Guide*. https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon240603_draftguide.en.pdf.

Faggionato, Giovanna, and Ben Munster. 2024. “Digital Euro Sparks Sovereignty Battle between EU Governments and ECB.” *Politico*, October 29, 2024. https://www.politico.eu/article/digital-euro-sparks-sovereignty-battle-eu-governments-ecb-monetary-tool-banking/.

Ferrari, Ms Valeria. 2022. “The Platformisation of Digital Payments: The Fabrication of Consumer Interest in the EU FinTech Agenda.” *Computer Law & Security Review* 45 (July):105687. https://doi.org/10.1016/j.clsr.2022.105687.

Feyen, Erik, Jon Frost, Leonardo Gambacorta, Harish Natarajan, and Matthew Saal. 2021. “Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy.” *Bank of International Settlements Papers* 117 (July). https://www.bis.org/publ/bppdf/bispap117.pdf.

Gil-Garcia, J. Ramon, and Miguel Á. Flores-Zúñiga. 2020. “Towards a Comprehensive Understanding of Digital Government Success: Integrating Implementation and Adoption Factors.” *Government Information Quarterly* 37 (4): 101518. https://doi.org/10.1016/j.giq.2020.101518.

Glasze, Georg, Cattaruzza ,Amaël, Douzet ,Frédérick, Dammann ,Finn, Bertran ,Marie-Gabrielle, Bômont ,Clotilde, Braun ,Matthias, et al. 2023. “Contested Spatialities of Digital Sovereignty.” *Geopolitics* 28 (2): 919–58. https://doi.org/10.1080/14650045.2022.2050070.

Goodell, John W. 2020. “COVID-19 and Finance: Agendas for Future Research.” *Finance Research Letters* 35 (July):101512. https://doi.org/10.1016/j.frl.2020.101512.

Goujard, Clothilde, and Laurens Cerulus. 2021. “Inside Gaia-X: How Chaos and Infighting Are Killing Europe’s Grand Cloud Project.” *Politico*, October 26, 2021, sec. Technology. https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/.

Hendrikse, Reijer, David Bassens, and Michiel van Meeteren. 2018. “The Appleization of Finance: Charting Incumbent Finance’s Embrace of FinTech.” *Finance and Society* 4 (2): 159–80. https://doi.org/10.2218/finsoc.v4i2.2870.

Hendrikse, Reijer, Michiel van Meeteren, and David Bassens. 2020. “Strategic Coupling between Finance, Technology and the State: Cultivating a Fintech Ecosystem for Incumbent Finance.” *Environment and Planning A: Economy and Space* 52 (8): 1516–38. https://doi.org/10.1177/0308518X19887967.

Hodson, Dermot, and Lucia Quaglia. 2009. “European Perspectives on the Global Financial Crisis: Introduction.” *Journal of Common Market Studies* 47 (5): 939–53. https://doi.org/10.1111/j.1468-5965.2009.02029.x.

Judt, Ewald, and Malte Krueger. 2021. “The European Payments Initiative: The next Big Thing in European Payments?” *Journal of Payments Strategy & Systems* 15 (3): 319–31.

Kaniadakis, Antonios, and Paige Foster. 2024. “The Role of Fintech Startups and Big Banks in Shaping Trust Expectations from Blockchain Use in Mainstream Financial Markets.” *Technological Forecasting and Social Change* 203 (June):123376. https://doi.org/10.1016/j.techfore.2024.123376.

Kindermann, Kornelius. 2024. “Drei Fragen und Antworten: Die Behördensoftware openDesk kommt.” *heise online*, October 4, 2024. https://www.heise.de/hintergrund/Drei-Fragen-und-Antworten-Die-Behoerdensoftware-openDesk-kommt-9961178.html.

Knafo, Sarah. 2025. “Draft Report on European Technological Sovereignty and Digital Infrastructure.” 2025/2007 (INI). European Parliament. https://www.europarl.europa.eu/doceo/document/ITRE-PR-768180_EN.pdf.

Kun, Eyup. 2024. “Challenges in Regulating Cloud Service Providers in EU Financial Regulation: From Operational to Systemic Risks, and Examining Challenges of the New Oversight Regime for Critical Cloud Service Providers under the Digital Operational Resilience Act.” *Computer Law & Security Review* 52 (April):105931. https://doi.org/10.1016/j.clsr.2023.105931.

Mano, Miguel de la, and Jorge Padilla. 2018. “Big Tech Banking.” *Journal of Competition Law & Economics* 14 (4): 494–526. https://doi.org/10.1093/joclec/nhz003.

Martin, Rosa. 2024. “Bizum and the Success of Instant Credit Transfers in Spain.” *Banco de Espagna Blog* (blog). March 21, 2024. https://www.bde.es/wbe/en/noticias-eventos/blog/bizum-y-el-exito-de-las-transferencias-inmediatas-en-espana.html.

Mohn, Augustinus, and Tom Barbereau. 2025. “Weerbare Systeeme” TNO.

Moloney, Niamh. 2010. “EU Financial Market Regulation after the Global Financial Crisis: ‘More Europe’ or More Risks?” *Common Market Law Review* 47 (5). https://doi.org/10.54648/cola2010058.

Munster, Ben. 2024. “The EU Wasted €60M on a Pointless Fintech Fad — but the Belgians Won’t Let It Die.” *Politico*, April 3, 2024. https://www.politico.eu/article/brussels-sunk-60-million-blockchain-money-rail-project-wont-call-quits-white-elephant-matthieu-michel/.

Ness, Susan. 2025. “Truth and Consequences: The Post-Election Regulatory Landscape for Big Tech.” *Tech Policy Press*, April 4, 2025. https://www.techpolicy.press/truth-and-consequences-the-postelection-regulatory-landscape-for-big-tech/.

OECD. 2020. “Digital Disruption in Banking and Its Impact on Competition.” OECD Competition Law and Policy Working Papers 243. https://www.oecd.org/en/publications/digital-disruption-in-banking-and-its-impact-on-competition_b8d8fcb1-en.html.

Pisa, Daan, Joris Vierhout, Amber Geurts, and Thijmen van Bree. 2024. “Grip Op Control Points.” R11817. TNO. https://vector.tno.nl/artikelen/grip-control-points-gerichter-innoveren/.

Prudential Regulation Authority. 2023. “Outsourcing and Third Party Risk Management.” Supervisory Statement. Bank of England. https://www.bankofengland.co.uk/paper/2023/ss/outsourcing-third-party-risk-management-ss-recognised-payment-system-operators.

Rankin, Jennifer. 2025. “EU Will Not Rip up Tech Rules for Trade Deal with Trump, Senior Official Says.” *The Guardian*, April 11, 2025, sec. World news. https://www.theguardian.com/world/2025/apr/11/eu-will-not-rip-up-tech-rules-for-trade-deal-with-trump-senior-official-says.

Rikap, Cecilia, Cédric Durand, Paolo Gerbaudo, Paris Marx, and Edemilson Paraná. 2024. “Reclaiming Digital Sovereignty: A Roadmap to Build a Digital Stack for People and the Planet.” The Bartlett Faculty of the Built Environment. https://www.ucl.ac.uk/bartlett/publications/2024/dec/reclaiming-digital-sovereignty.

Rojszczak, Marcin. 2020. “CLOUD Act Agreements from an EU Perspective.” *Computer Law & Security Review* 38 (September):105442. https://doi.org/10.1016/j.clsr.2020.105442.

Sandbu, Martin. 2025. “The Battle for the Global Payments System Is under Way.” *Financial Times*, April 6, 2025. https://www.ft.com/content/40f6e292-839c-4d1f-994e-59bed627b909.

Stefanelli, Valeria, and Francesco Manta. 2023. “Digital Financial Services and Open Banking Innovation: Are Banks Becoming ‘Invisible’?” *Global Business Review*, May. https://doi.org/10.1177/09721509231151491.

Stolwijk, Claire, Matthijs Punter, Tjerk Timan, Frank Berkers, Ilina Georgieva, Rick Gilsing, Harrie Bastiaansen, et al. 2022. “Bridging the Dutch and European Digital Sovereignty Gap.” TNO 2022 R10507. TNO. https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf.

Stolwijk, Claire, Matthijs Punter, Paul Timmers, Julian Rabbie, David Regeczi, and Simon Dalmolen. 2024. “Towards a Sovereign Digital Future – the Netherlands in Europe.” TNO. https://vector.tno.nl/en/articles/digital-transformation-europe/.

Sveriges Riksbank. 2024. “Payments Report 2024.” Sveriges Riksbank. https://www.riksbank.se/globalassets/media/rapporter/betalningsrapport/2024/engelsk/payments-report-2024.pdf.

Toffaletti, Sebastiano. 2025. “European Industry Demands Eurostack to Power EU Competitiveness.” *European DIGITAL SME Alliance* (blog). March 17, 2025. https://www.digitalsme.eu/european-industry-demands-a-eurostack-to-power-eu-competitiveness/.

Trigt, Marjolein van. 2025. “Amsterdam Presenteert Plan Voor Digitale Autonomie.” *Binnenlans Bestuur*, March 18, 2025, sec. Digitaal. https://www.binnenlandsbestuur.nl/digitaal/amsterdam-presenteert-plan-voor-digitale-autonomie.

Vaughan-Nichols, Steven. 2025. “Why Denmark Is Dumping Microsoft Office and Windows for LibreOffice and Linux.” *ZDNET*, June 11, 2025. https://www.zdnet.com/article/why-denmark-is-dumping-microsoft-office-and-windows-for-libreoffice-and-linux/.

Vigliarolo, Brandon. 2025. “Time to Ditch US Tech for Homegrown Options, Says Dutch Parliament.” *The Register*, March 19, 2025. https://www.theregister.com/2025/03/19/dutch_parliament_us_tech/.

Westermeier, Carola. 2020. “Money Is Data – the Platformization of Financial Transactions.” *Information, Communication & Society* 23 (14): 2047–63. https://doi.org/10.1080/1369118X.2020.1770833.

———. 2024. “The Digital Euro: A Materialization of (in)Security.” *Review of International Political Economy* 31 (5): 1569–92. https://doi.org/10.1080/09692290.2024.2345613.

Xiong, Xiong, Jin Zhang, Xi Jin, and Xu Feng. 2016. “Review on Financial Innovations in Big Data Era.” *Journal of Systems Science and Information* 4 (6): 489–504. https://doi.org/10.21078/JSSI-2016-489-16.

Zachariadis, Markos, and Pinar Ozcan. 2016. “The API Economy and Digital Transformation in Financial Services: The Case of Open Banking.” *SWIFT Institute Working Paper* 2016 (1). https://doi.org/10.2139/ssrn.2975199.

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag

tno.vector.nl