• FINANSE I PRAWO FINANSOWE •
• JOURNAL OF FINANCE AND FINANCIAL LAW •

grudzień / december 2025 • vol. 4(48): 57–86
https://doi.org/10.18778/2391-6478.4.48.03

COPE Member since 2021 JM15102

Michał Włodarczyk https://orcid.org/0000-0001-9913-521X
Department of Risk Management and Insurance, Cracow Univerisity of Economics ,
e-mail: wlodarcm@uek.krakow.pl

TECHNOLOGICAL SOVEREIGNTY AND THE STABILITY OF THE EUROPEAN FINANCIAL SECTOR IN THE ERA OF ARTIFICIAL INTELLIGENCE

ABSTRACT

The purpose of the article The article aims to develop a composite index of technological sovereignty for EU member states and examine its relationship with systemic financial stress. It highlights technological dependencies as a potential source of systemic risk.

Methodology The study covers 16 EU countries. Six indicators on infrastructure, AI and cloud adoption, and ICT capacity were standardised and weighted using an optimisation procedure (SLSQP). The index for 2023 was compared with CISS values from February 2025. Correlation analysis was applied to assess relationships between index components and systemic stress.

Results of the research Northern and Western EU countries scored highest on technological sovereignty, while Southern and Eastern states lagged behind. AI and cloud adoption correlate positively with systemic stress, whereas infrastructural and human capital indicators show weaker or stabilising effects. Technological dependencies emerge as an overlooked dimension of systemic risk.

Keywords: AI, risk management, vendor lock-in, digital economy

JEL Class: O33, F52, L86

Received: 30.06.2025. Accepted: 20.10.2025.

Funding information: The article presents the result of the Project no 030/EFZ/2023/POT financed from the subsidy granted to the Krakow University of Economics. **Conflicts of interests:** None. **Ethical considerations:** The Author assure of no violations of publication ethics and take full responsibility for the content of the publication.

Indtroduction

The rapid development of artificial intelligence (AI) is profoundly transforming financial systems, enhancing processes ranging from credit scoring to algorithmic trading, while simultaneously introducing new sources of systemic risk. According to the Global Financial Stability Report (IMF, 2024), AI has the potential to amplify the procyclical behavior of markets during periods of stress, acting as a catalyst for turbulence rather than a stabilizing buffer.

In the meantime, the financial sector is becoming increasingly dependent on a small group of cloud and algorithmic service providers, leading to infrastructural concentration and vendor lock-in, which in turn heightens the risks associated with limited technological control — particularly in the context of geopolitical tensions. In this regard, technological sovereignty emerges as a key dimension of macro-financial resilience, understood as the capacity to independently develop, deploy, and govern digital technologies within strategic sectors.

The purpose of this article is to examine how the lack of technological sovereignty in the field of AI affects the level of systemic stress in the financial sectors of EU countries. This is achieved by constructing a technological sovereignty index and comparing it with the CISS (Composite Indicator of Systemic Stress) developed by the European Central Bank.

Literature

The concept of digital sovereignty emerged in the 1990s in response to the dominance of US Internet companies (Cong & Thumfart, 2022; Glasze et al., 2023), gaining prominence with the politicization of technology in the late 1910s. The French concept of *souveraineté numérique* in 2012 was a reaction to the U.S. reliance on technology (Musiani 2013; Thumfart 2022), and the Snowden revelations in 2013 sparked a debate about technological independence

in Germany (Pohle, 2020; Glasze et al., 2023). The turning point came in 2016 with the election of Donald Trump and the trade war with China.

At the EU level, the acceleration of legislative action (RODO, Digital Markets Act, Digital Services Act, AI Act) was part of the definition of digital sovereignty as an element of strategic autonomy (European Council, 2021), understood as the ability to act independently and protect infrastructure (Madiega, 2020). The contemporary debate emphasizes its character as a political construct legitimizing the technological practices of various actors (Pohle et al., 2025), and the concept of "unthinking digital sovereignty" postulates a shift from a state-centric view to an analysis of its relational, historical and negotiated aspects.

Technological sovereignty goes beyond ownership of infrastructure and digital competencies to include the ability to shape rules and standards in the areas of data, AI and platforms, with its meaning varying regionally, with Europe emphasizing democratic values and individual rights and China emphasizing defense against external interference (Creemers, 2020; Pohle et al., 2025). In the face of the dominance of global technology corporations, reflection is needed on the mechanisms of control and accountability of these new forms of power.

At the same time, the development of AI as a general-purpose technology – comparable to electrification or the Internet (Brynjolfsson & McAfee, 2017) – is increasing the financial sector's dependence on US and Chinese cloud services. This dependence becomes particularly important in the context of geopolitical tensions and deglobalization, fostering nearshoring, EU strategic autonomy or Chinese digital protectionism (Zuboff, 2019; Pohle & Thiel, 2020).

Meanwhile, Europe is lagging behind in terms of technology leaders – most financial data and AI algorithms are processed in US clouds (Bria, 2015). The cloud market is dominated by Amazon AWS (30%), Microsoft Azure (21%) and Google Cloud (12%), while Alibaba has only a 4% share (Statista, 2025). In

GPU manufacturing, NVIDIA controls 92% of the market, and together with AMD and Intel, the share of American companies reaches 97% (Fernandez, 2025). The lack of European giants is also evident in consumer electronics, where U.S. brands (Apple, 26%) and Chinese brands (Xiaomi, Motorola, Oppo; 25%) dominate, completely displacing European products (Canalys, 2025).

Lack of in-house infrastructure and limited ability to develop national or EU AI models generate systemic risks. The IMF (2024) points out that mass deployment of AI in finance increases system complexity, reduces transparency of decisions and hinders oversight, and in a crisis can amplify market panic. Additionally, the dominance of a few global cloud and AI providers (vendor lock-in) creates structural operational vulnerabilities, susceptible to exploitation in political conflicts or cyber attacks (DeNardis, 2014; IMF, 2024).

One of the key challenges of the digital transformation of the financial sector is vendor lock-in, or dependence on a single cloud and algorithmic service provider. Limited interoperability, lack of open standards and difficulties in migrating data or AI models tie institutions to specific platforms, limiting flexibility and increasing the risk of switching costs (Opara-Martins et al., 2016). The problem is exacerbated by limited awareness of the risks – 71% of companies cite vendor lock-in as a barrier to further migration (Opara-Martins et al., 2016) – and increasing reliance on third-party AI solutions (Soetan, 2023). Lack of control over data is becoming a significant systemic risk (Adeyelu et al., 2024), and for the EU it means limited ability to intervene in crises and protect consumers, making technological sovereignty a condition for financial stability.

The EU has increased funding for cyber security to €2.9 billion in IFF 2021–2027, a 200% increase over the previous period, but still small compared to the US budget ($13 billion in 2025) (PEI, 2025). Similarly, in AI investment, the EU ($10 billion in 2023) is clearly behind China ($18 billion) and the US

($90 billion) (OECD GPAI, 2025). However, without its own large language models, chip manufacturing and cloud technologies, even increased spending will go mainly to US companies. As a result, in line with the vendor lock-in phenomenon, increased productivity will reinforce dependence on external suppliers, creating a closed circle that limits the growth of European technology companies and threatens the sovereignty and stability of the financial sector.

Recent studies point to three main channels for AI to transfer systemic risk: homogeneous machine learning models fostering herding by design (Danielsson, Uthemann & Macrae 2024), concentration of operational risk in hyperscale cloud providers (Opara-Martins, 2016), and vulnerability to failure of individual SaaS components, as exemplified by the failure of CrowdStrike in 2024 (Douglas, 2024).

At the same time, the concept of digital sovereignty has expanded to include infrastructural, regulatory and competency dimensions (Fratini et al, 2024). Lack of control over the AI-cloud layer limits the ability of states to respond to crises, even with extensive data infrastructure (Fratini, 2024; Mügge, 2025). The degree of technological sovereignty acts as a moderator of systemic stress, increasing its level in countries with lower sovereignty.

Despite growing interest, systematic, empirical analyses of the links between AI, systemic risk and financial stability are lacking. Current indicators (DESI, AI Readiness Index) do not take into account control of computing infrastructure or crisis response capabilities, making it difficult to quantify technological sovereignty and its impact on macrofinancial resilience.

In the context of the growing use of AI and cloud solutions in finance, the key question becomes whether their intensification without ensuring an adequate level of technological autonomy increases systemic risk. This is indicated both by reports from the IMF, ECB and OECD, as well as empirical

cases revealing the vulnerability of digital infrastructure to disruption, such as the CrowdStrike crash in 2024.

The paper attempts to empirically verify this relationship by constructing an index of technological sovereignty for European Union member states and comparing its value with the CISS systemic stress index developed by the European Central Bank. The study aims to answer the following questions:

1. Is there a relationship between the overall level of technological sovereignty and the level of systemic stress in the financial sector of EU countries?
2. Which components of sovereignty (infrastructure, competence, use of technology) show a significant impact on the level of systemic stress?
3. Can the intensive use of artificial intelligence and cloud computing be associated with increased levels of systemic stress, regardless of the overall level of technological sovereignty?

Based on the above questions, the following research hypotheses were formulated:

- **H1**: There is a significant relationship between the overall level of technological sovereignty and the level of systemic stress in the financial sector.
- **H2a**: A high percentage of companies using artificial intelligence correlates positively with the level of systemic stress.
- **H2b**: A high percentage of enterprises using cloud computing correlates positively with the level of systemic stress.
- **H2c**: High share of ICT sector in GDP and high saturation of data center infrastructure (per capita) correlate negatively with the level of systemic stress.

- **H3**: The impact of intensive use of AI and cloud on the level of systemic stress is stronger in countries with lower levels of technological sovereignty.

Against this theoretical and conceptual background, the next section presents the empirical design of the study. It outlines the construction of the technological sovereignty index and explains how it is linked with systemic stress indicators to address the research questions formulated above.

Methodology

The analysis used a taxonomic method, which allows for the construction of a synthetic index of technological sovereignty based on a set of quantitative socio--economic variables. It was enriched with a comparative analysis of variables related to digital sovereignty.

The taxonomic method was chosen for its ability to aggregate multidimensional information into a one-dimensional synthetic index, while maintaining comparability across units of analysis. This method has previously been used in the literature to at least measure digital saturation (Dykas, Koscielniak & Tokarski, 2013) and to build comparative composite indices. In the study, it was assumed that all variables are stimulants, and therefore their higher values indicate a higher level of technological sovereignty. The variables were subjected to standardization.

The analysis covered the 27 member states of the European Union, and the time range of the input data was 2023. This year was chosen as the most recent period with available comparable statistics from the area of digital technology use and cloud infrastructure in the EU. The dataset on the number of data centers was dynamic and indicated only the current state which prevented the author from analyzing the dynamics.

The construction of the Technological Sovereignty Index (TSI) is based on six standardized quantitative indicators capturing key infrastructural, technological, and competency-related dimensions of digital sovereignty. Each variable was selected on the basis of data availability, comparability across EU member states, and its theoretical relevance to technological control and financial stability. Importantly, the indicators reflect different aspects of the phenomenon and are subject to specific interpretative limitations, which are:

- Number of data centres per 1,000 inhabitants

  This indicator reflects the degree of physical digital infrastructure saturation, which is a prerequisite for hosting and processing data within a country's jurisdiction. A higher number of data centres per capita suggests greater local computing capacity and, potentially, higher autonomy in storing and processing financial data. However, this measure does not account for ownership structure or operational control: many centres located in the EU are operated by foreign corporations. Moreover, data centres typically serve transnational markets and do not necessarily scale with population size. Consequently, this variable should be interpreted as a proxy for infrastructural presence rather than actual sovereignty.
- Number of cloud facilities per 1,000 inhabitants

  This variable captures the availability of cloud infrastructure services within national borders, encompassing public, private, and hybrid models. Its relevance lies in the centrality of cloud infrastructure for AI deployment, financial data management, and critical services. Similar to data centres, this indicator does not reflect the degree of domestic control or interoperability standards. The presence of foreign-operated hyperscale cloud facilities can in fact increase dependence on non-EU providers, underscoring the need for careful interpretation.

- Percentage of enterprises using artificial intelligence

  This measure reflects the diffusion of AI technologies[1] in the economy and, in particular, in the financial sector. While widespread AI adoption may indicate technological advancement, it does not capture who owns, develops, or governs these systems. Many commercial AI solutions are provided by foreign vendors, creating operational and legal dependencies. Furthermore, not every technology reported by enterprises as "AI" constitutes advanced or systemic AI within the meaning relevant for financial stability. This indicator should therefore be seen primarily as a measure of technological uptake rather than of sovereign capability.

- Percentage of enterprises using cloud computing[2]

  Analogous to AI usage, this variable reflects the intensity of cloud adoption across the enterprise sector. While cloud computing can enable scalability and innovation, dependence on foreign hyperscale providers introduces systemic vulnerabilities (e.g., vendor lock-in, jurisdictional fragmentation, or data localisation issues). The indicator captures adoption levels but does not measure the degree of control over cloud layers, making it necessary to complement it with infrastructural and regulatory considerations.

[1] Share of enterprises with ≥ 10 employees that used at least one artificial intelligence technology (e.g. machine learning/deep learning, image/text/speech recognition or analysis, natural language generation, autonomous systems or AI-based RPA). Definition and measurement follow Eurostat's *ICT usage and e-commerce in enterprises* survey. Dataset: isoc_eb_ai (and sectoral variant isoc_eb_ain2)."

[2] Share of enterprises with ≥ 10 employees that purchased cloud computing services (SaaS/IaaS/PaaS) delivered over the internet by external providers; services are characterised by on-demand self-service, flexible scalability, and pay-per-use pricing. Definition and measurement follow Eurostat's *ICT usage and e-commerce in enterprises* survey. Dataset: isoc_cicce_use (and sectoral variant isoc_cicce_usen2).

- Share of the ICT sector in gross domestic product

  This indicator represents the economic weight of the ICT sector in the national economy, capturing the structural embedding of digital activities and technological competencies. A higher share may indicate stronger endogenous capabilities to develop, maintain, and govern digital infrastructure. However, this variable does not directly measure ownership or strategic control, and should be interpreted as a complementary economic dimension of sovereignty.

- Percentage of enterprises employing ICT specialists

  This measure reflects the availability of human capital and technical skills necessary to support digital infrastructure, develop domestic solutions, and maintain operational autonomy. While essential for sovereignty, the indicator alone does not account for the direction of technological development or the presence of domestic versus foreign platforms.

Taken together, these six indicators offer a multi-dimensional view of technological sovereignty, encompassing infrastructure, adoption, and competencies. At the same time, it is crucial to distinguish between digital adoption and technological control: high levels of AI and cloud use do not automatically imply sovereignty and may, under certain conditions, increase exposure to systemic risk. The selection of these variables reflects a balance between theoretical relevance and data availability, but the interpretation of results must account for the limitations outlined above.

The weights for each variable were estimated using the Sequential Least Squares Programming (SLQP) nonlinear optimization method, using the scipy.optimize library in Python. A function was used to minimize the sum of relative errors, assuming that the sum of the weights equals 1 and that each weight

falls within the interval [0,1]. This approach provides both methodological transparency and the ability to account for the internal structure of the data.

The taxonomic index values of technological sovereignty (TSI) for each country were determined as a linear combination of the sum of the products of the values of each standardized variable and their weights (Equation 1).

$$TSI_t^i = \omega_1 Z_{i,1} + \omega_2 Z_{i,2} + \omega_3 Z_{i,3} + \cdots + \omega_6 Z_{i,6} \quad (1)$$

An alternative option, based on Hellwig's measure of distance from the development pattern, was considered at the sensitivity testing stage; however, the form (1) was chosen because it has less sensitivity to extreme observations and retains full interpretability of the weights as information shares of the variables.

The choice of a taxonomic method was preceded by an analysis of alternative approaches, such as principal component analysis (PCA), expert approaches and ready-made aggregate indicators (e.g. DESI, AI Readiness Index). These methods, while widely used, come with significant limitations: PCA generates components that are difficult to interpret directly, expert approaches are characterized by arbitrariness, and administrative indicators focus mainly on digitization, leaving out aspects of infrastructure and jurisdictional sovereignty.

The taxonomic method was chosen as a solution that allows for transparent aggregation of standardized quantitative data, preservation of control over the weighting structure, and the possibility of comparative analysis of EU countries, taking into account the complexity of the phenomenon. Its application is also confirmed by previous research on digital development and institutional resilience.

Macroeconomic input variables used to construct the Technological Sovereignty Index refer to the most recent period with comparable Eurostat

statistics available for all EU member states. The CISS values and number of data centers and cloud infrastructure come from February 2025, reflecting the latest data available at the time of analysis. The study therefore applies a cross-sectional design, comparing sovereignty levels at time *t* with systemic stress observed approximately two years later (*t+2*). This temporal structure allows for the possibility that structural characteristics of technological sovereignty precede and influence financial stress dynamics, but it does not capture full time-series effects. In the robustness checks, alternative specifications with lagged relationships were explored to account for potential timing discrepancies between index components and financial stress indicators.

To assess the robustness of the Technological Sovereignty Index (TSI), several complementary checks were carried out. First, an alternative aggregation procedure based on Hellwig's measure of distance from the development pattern was applied. This method, commonly used in taxonomic analyses, yielded country rankings and relationships with systemic stress that were highly consistent with the baseline index, confirming that the main results are not driven by the chosen aggregation formula.

Second, the temporal alignment between variables and financial stress indicators was examined. The TSI is based on data for 2023, while CISS values refer to February 2025, effectively introducing a two-year lag. This structure allows for a basic robustness check regarding timing: technological sovereignty indicators precede the observed levels of systemic stress. The results remain unchanged under this alignment.

In addition, simple alternative specifications, such as equal-weighted aggregation and the exclusion of individual variables, were explored. These did not materially alter the country ordering or the direction of the relationships

observed. Taken together, these tests indicate that the results are stable and not dependent on a single modelling assumption.

Results

The flywheel of the Fourth Industrial Revolution, and therefore the digital economy, is virtual data. Their creation, analysis and processing are what hydrocarbon extraction and steel production used to be. Analyzing the countries with the greatest potential for "digital thinking" i.e., computing power as seen in Table 1, the dominance of the US is evident. Even after adding up the results of the countries of Europe (Italy, Switzerland, Germany, Finland, Spain, France, the Netherlands and the UK), they reach only 43% of the computing power of the United States.

Table 1

Estimated computing power and number of country based on TOP500 supercomputer ranking in November 2024 (in TFlops)

Country	# of supercomputers in TOP500	Estimated computing power in TFlops
USA	172	6500000
Japan	34	941000
Italy	13	838000
Switzerland	5	474000
Germany	41	405000
Finland	3	391000
China	63	319000
Spain	3	222000
South Korea	13	213000
France	24	298000

Country	# of supercomputers in TOP500	Estimated computing power in TFlops
Taiwan	7	104000
Netherlands	10	98000
Saudi Arabia	7	96000
United Kingdom	14	85000
Russia	6	71000
Other	84	697000

Source: Own compilation based on Voronoi (2025).

Supercomputers are an indicator of investments made in digital infrastructure. A similar indicator could be data centers – special storage facilities that process and manage digital data. This is the infrastructure needed to develop and train artificial intelligence algorithms, and therefore a strategic element of the economy's security. For this purpose, a spatial analysis of EU countries was made in terms of the number of functioning data centers as well as cloud service providers (public, private and hybrid clouds) for March 2025 presented in Table 2.

Table 2

Values of factors used in the Technological Sovereignty Index

Country	Data centers [2025]	Cloud infrastructure [2025]	AI usage by enterprises in % [2024]	Cloud usage in % [2023]	ICT % GDP [2022]	Enterprises that employ ICT specialists in % [2024]
Austria	45	4	20.27	46.48	3.83	19.91
Belgium	47	5	24.71	51.69	4.08	29.11
Bulgaria	30	6	6.47	17.5	7.42	17.81
Croatia	15	4	11.76	45.08	5.32	15.89
Cyprus	18	3	7.9	52.93	10.42	27.48

Country	Data centers [2025]	Cloud infrastructure [2025]	AI usage by enterprises in % [2024]	Cloud usage in % [2023]	ICT % GDP [2022]	Enterprises that employ ICT specialists in % [2024]
Czechia	49	4	11.26	47.15	4.93	20.2
Denmark	55	2	27.58	69.48	3.81	30.94
Estonia	12	0	13.89	58.57	5.97	19.22
Finland	50	5	24.37	78.29	5.81	30.51
France	254	19	9.91	26.76	4.36	15.94
Germany	416	33	19.75	47	4.77	22.86
Greece	19	8	9.81	23.59	3.04	22.53
Hungary	16	1	7.41	44.94	5.48	29.34
Ireland	99	9	14.9	63.1	34.78	30.28
Italy	164	10	8.2	61.39	3.21	12.44
Latvia	22	3	8.83	35.76	6.45	17.99
Lithuania	14	3	8.76	38.39	4.59	16.12
Luxembourg	13	2	23.73	37.04	5.67	23.35
Malta	7	1	17.3	66.74	10.14	34.11
Netherlands	191	21	23.06	64.19	5.31	29.73
Poland	83	8	5.9	55.67	4.03	25.99
Portugal	41	3	8.63	37.5	4.47	20.56
Romania	59	4	3.07	18.4	4.44	13.16
Slovakia	13	2	10.78	34.42	4.47	17.25
Slovenia	20	0	20.89	40.21	4.3	17.71
Spain	152	11	11.31	30.04	3.55	14.57
Sweden	95	2	25.09	71.62	6.24	21.6

Source: Data Center Map (2025); Eurostat (tin00074, isoc_eb_ai, isoc_cicce_use, isoc_ske_itspen2).

The largest number of data centers is in Germany (416), France (254), the Netherlands (191) and Italy (164). EU countries together have 1999 such centers. By comparison, major rivals have respectively:

- United Kingdom 404;
- Japan 180;
- India 259;
- China 432;
- United States 3648.

However, it is important to make the results more realistic by dividing them by the population in thousands to measure the saturation of data centers. By this measure, it turns out that only four EU countries have a higher score than the US (Luxembourg, Ireland, Malta and Latvia). The average for EU countries is 0.0067 data centers per 1,000 inhabitants, while the figure for the US is 0.0109.

In the case of cloud-enabled centers, the EU has 173 facilities, while competitors respectively:

- UK 45;
- Japan 5;
- India 14;
- China 12;
- United States 128.

This would indicate a strong position, especially when analyzing the number per 1,000 inhabitants, where the Union scores 0.0007 and the United States 0.0004.

The initial goal was to analyze the data centers present in EU countries by their origin, to divide them into domestic, European and foreign. Unfortunately, through difficulties in the availability of such data and in verifying the shareholding of many companies, a decision was necessary to

outline the location of data centers of the largest digital companies from the US and China.

In the case of US companies, it is as follows:

- Meta: three centers (Ireland, Denmark, Sweden) (Meta, 2025);
- Alphabet: 10 centers (Finland, Denmark, Germany, Netherlands, Belgium, Ireland) (Google, 2025);
- Amazon: 32 centers (Spain, Ireland, Sweden) (Amazon, 2025)
- Apple: one center (Denmark) (Apple, 2025).

In contrast, analysis of Chinese giants such as Alibaba and Tencent indicates sovereignty in the Chinese edition. None of these companies' 15 data centers are located outside the PRC (Tencent; Alibaba, 2025). However, China Telecom (the world's largest telco) works with more than 180 data centers worldwide. Significantly, and demonstrating the low transparency of the Chinese market, China Telecom claims on its website that it operates more than 450 data centers in China – despite the fact that even counting Macau and Hong Kong, they do not currently have that many (according to official data) (China Telecom, 2025).

The estimated weights for taxonomic index of technological sovereignty obtained the following values:

- Number of data centers per 1,000 residents – 0.142;
- Number of cloud facilities per 1,000 residents – 0.1433;
- Share of companies using artificial intelligence – 0.1379;
- Share of companies using cloud computing – 0.1706;
- Share of ICT sector in GDP – 0.2094;
- Share of companies employing ICT specialists in total employment – 0.1968.

Table 3

Value of the index of technological sovereignty and CISS

Country	Technological Sovereignty Index	CISS
Austria	0.3974	0.1778
Belgium	0.4780	0.1145
Bulgaria	0.2962	–
Croatia	0.3585	–
Cyprus	0.5801	–
Czechia	0.3557	0.0161
Denmark	0.5741	0.3306
Estonia	0.4077	–
Finland	0.6114	0.1575
France	0.2664	0.0649
Germany	0.4171	0.0448
Greece	0.2987	0.0193
Hungary	0.3544	0.0261
Ireland	0.8129	0.0189
Italy	0.2942	0.158
Latvia	0.4263	–
Lithuania	0.3335	–
Luxembourg	0.6535	–
Malta	0.6684	–
Netherlands	0.5925	0.1436
Poland	0.3519	0.1031
Portugal	0.3122	0.0306
Romania	0.1907	–

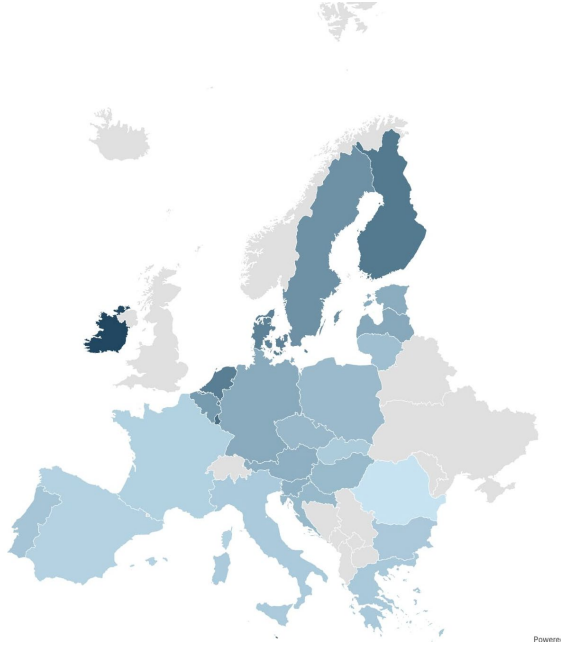
Country	Technological Sovereignty Index	CISS
Slovakia	0.2904	–
Slovenia	0.3888	–
Spain	0.2612	0.0401
Sweden	0.5184	0.11

Source: Own elaboration and European Central Bank (2025).

Analyzing the index values, it is possible to conclude that Ireland, Malta, Luxembourg and Finland have the highest digital sovereignty. In contrast, Romania, Spain, France and Slovakia have the lowest.

Figure 1

The level of the index of technological sovereignty in the analyzed countries



Source: Own study.

The Composite Indicator of Systemic Stress (CISS) index was used to measure the stability of a country's financial sector. This is an index developed by the European Central Bank (ECB) to monitor the level of systemic stress in the eurozone financial system. Its design is based on an analysis of five key financial market segments: the money market, the bond market, the stock market, the foreign exchange market and the financial intermediary sector. For each of these segments, sub-indices are calculated based on three raw measures of stress, such as price volatility, yield spreads and liquidity ratios. A total of 15 measures are used, which, after appropriate statistical transformation, are aggregated with time-varying correlations between the sub-indexes. As a result, the CISS assigns more weight to situations where stress occurs simultaneously in multiple market segments, reflecting its systemic nature. The index takes values in the range of (0,1), where a lower value indicates low volatility, consistency of market segments and overall stability. As the value of the index increases, stability decreases and more frequent sharp changes in asset prices are possible (Hollo, Kremer & Lo Duca, 2012).

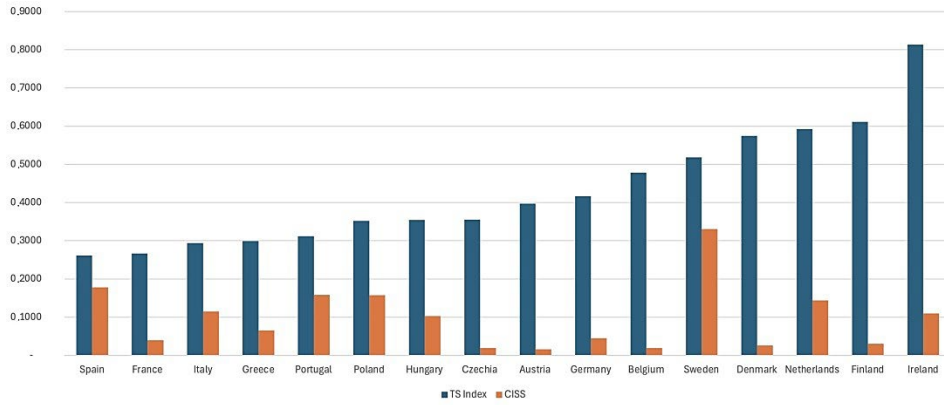
The most recent monthly data for EU countries at the time of the study was used. Data for February 2025 for 16 national financial markets can be seen in Table 3. The result for Bulgaria, Croatia, Cyprus, Estonia, Latvia, Lithuania, Luxembourg, Malta, Romania, Slovakia and Slovenia is not presented due to lack of available data.

An analysis of Table 3 shows a wide variation in the stability of national financial sectors. The highest value, and therefore the least stable market, is Denmark, Austria and Italy. In contrast, the Czech Republic, Ireland and Greece proved to be the most stable. At the same time, there is no apparent trend as to the higher stability of Eurozone countries. Two countries with moderate results are Poland and Sweden, countries with their own currencies. This may indicate

that the common currency is not the dominant factor in the case of sector stability.

Figure 2

Comparison of the values of the technological sovereignty index and the CISS for the countries analyzed



Source: Own study.

Pearson's correlation coefficient for the two indices was 0.0072, which indicates that there is no clear connection between the two values. The author analyzed the correlation of the various variables used to build the digital sovereignty index, obtaining the following values:

- Number of data centers per 1,000 residents: 0.186;
- Number of cloud facilities per 1,000 residents: −0.089;
- Share of companies using artificial intelligence: 0.622;
- Share of companies using cloud computing: 0.589;
- Share of ICT sector in GDP: −0.257;
- Share of companies employing ICT specialists in total employment: 0.254.

Table 4

Comparison of correlation values between the component factors of the Technological Sovereignty Index and the CISS

Component	r (Pearson)	p-value	Interpretation
Use of AI [% of companies]	0.622	0.00014	Strong positive correlation, statistically significant
Cloud usage [% of companies]	0.589	0.00039	Strong positive correlation, statistically significant
ICT in GDP [%]	−0.257	0.155	Negative correlation, not significant
Data centers / 1,000 people	0.186	0.307	Weak positive correlation, not significant
Cloud facilities / 1000	−0.089	0.63	No correlation

Source: Own study.

The correlation analysis between the components of the technological sovereignty index and the CISS index reveals that not all variables have a neutral or stabilizing effect on the financial sector. On the contrary, the high use of artificial intelligence and cloud services by companies is associated with a marked increase in the level of systemic stress. This may reflect increased vulnerability of the system to shocks, automation of pro-cyclical decisions or lack of control over the operating model. Thus, technological sovereignty should not be equated solely with the level of digitization, but with the quality of control and ability to manage modern infrastructure.

Conclusions

The analysis confirms that technological sovereignty in AI can be an important component of macro-financial resilience, but it is not a clear-cut or unidimensional phenomenon. The Pearson correlation coefficient between the

sovereignty index and the CISS index was only 0.007, indicating that there is no statistically significant linear relationship between these variables. The results suggest that digital infrastructure alone is a necessary but not sufficient condition for financial stability.

A detailed analysis showed that variables related to the use of AI (+0.622) and cloud computing (+0.589) have the strongest positive correlation with CISS, which may reflect the risks posed by the automation of decisions, limited auditability of models and dependence on external vendors (vendor lock-in). In a crisis, these technologies may amplify shocks rather than cushion them. In contrast, the ICT sector's share of GDP (−0.257) and the number of data centers per 1,000 residents (0.186) showed a weak but stabilizing trend, suggesting that deeper embedding of digital competencies in the economy may act as a buffer against external shocks.

Based on the analysis, several directional recommendations were made for public policy in the area of digital sovereignty. First, building digital resilience should take into account not only the presence of infrastructure, but also real control over it – especially the ownership of EU entities. Second, the assumption that heavy use of AI and cloud without local control promotes stability should be reviewed, as without auditability, interoperability and strategic independence, it can increase systemic stress. Third, the EU should consider creating "digital macrostability" indices that measure systemic risk from automation, vendor lock-in and technology dependency, such as in the framework of EBA or FSAP activities. Fourth, the indices should take into account the ownership structure of digital infrastructure, determining the share of AI and clouds under the control of EU versus non-EU entities. Finally, digitization strategies should be synchronized with macroeconomic policies, treating AI development not just

as an innovation, but as a strategic resource, crucial to the ability to intervene effectively in a crisis.

The sample covers 16 EU countries with CISS availability during the analyzed period. The limited sample size and lack of full geographic coverage suggest caution in generalizing the results across the EU. The presented relationships should be considered as indicative of trends, not as universal evidence. In addition, the analysis is cross-sectional, comparing technological sovereignty levels in 2023 with systemic stress in early 2025. While this design provides useful insights into temporal ordering, it does not capture dynamic feedback effects over time.

A methodological limitation is that two of the six index variables (AI and cloud usage) reflect technology adoption rather than direct control, potentially blurring the distinction between structural sovereignty and the diffusion of foreign technologies. Moreover, integrating digital sovereignty indicators into macroprudential frameworks may face practical barriers related to data availability, differences in national capacities, and the cross-border nature of digital infrastructures. Future research should address these issues by developing alternative index specifications, using panel data to analyse dynamic relationships, and incorporating more granular indicators of ownership and control.

Discussion

The results undermine the prevailing assumption in the literature that the increase in digitization and use of AI automatically strengthens the systemic resilience of countries. Popular indexes, such as the AI Readiness Index or the Digital Economy and Society Index (Oxford Insights, 2023; European Commission, 2023), measure the degree of digitization and AI adoption as indicators of "digital readiness," assuming their positive impact on stability. Meanwhile, the analysis indicates that intensifying the use of AI and cloud

computing in an environment of limited infrastructure and competency control can increase systemic stress – this is supported by high positive correlations with CISS for the share of companies adopting AI (r = 0.622) and cloud (r = 0.589), as well as incidents of failure with cascading effects, such as CrowdStrike in 2024 (George, 2024).

The study proposes complementing the dominant normative-legal approaches (Pohle and Thiel, 2020) with an infrastructural and operational dimension, showing that digitization alone does not provide resilience without control over data localization, system interoperability and independence from foreign providers. In this sense, this approach fits in with the critique of the "de-sovereigntization" of digital infrastructure and the concept of technological neutrality of AI progress (Srivastava & Bullock, 2024). Technological sovereignty appears here not as an element of strategic ambitions, but as a prerequisite for the state's ability to respond to crises and limit contagion effects in complex financial systems.

An important practical consideration concerns the implementation barriers for the proposed digital macrostability indicators. While the results highlight the relevance of technological sovereignty for financial stability, integrating these indicators into existing macroprudential frameworks may be constrained by limited data availability, differences in national statistical capacities, and the cross-border nature of digital infrastructures. In particular, dependencies on non-EU technology providers complicate monitoring and regulatory oversight. Addressing these challenges would require improved data collection, harmonisation across EU member states, and closer coordination between financial supervisors and digital regulators.

Summary

The article assesses the impact of the level of technological sovereignty of EU countries on systemic stress in the financial sector, using the synthetic index and CISS data. Although no clear correlation was found between the overall level of sovereignty and the CISS, the analysis revealed that intensive use of AI and cloud computing – in the absence of local control – is associated with higher levels of systemic stress, suggesting vulnerability to disruption.

The study has limitations: cross-sectional nature (year 2023), limited sample of countries with CISS data availability, lack of consideration of qualitative differences in AI applications and cloud ownership structure. The results underscore the need for qualitative control of digital infrastructure in digitization policies and financial regulations, and the development of open, local and interoperable technology ecosystems appears as a tool for strengthening systemic stability, not just as an element of digital sovereignty.

References

Adeyelu, O., Ugochukwu, C.E., Shonibare, M.A. (2024). Automating financial regulatory compliance with AI: A review and application scenarios. *Finance & Accounting Research Journal*, 6(4): 580–601, https://doi.org/10.51594/farj.v6i4.1035

Alibaba. (2025). www.datacentermap.com/c/alibaba-cloud

Amazon. (2025). www.datacentermap.com/c/amazon-aws

Apple. (2025). www.datacentermap.com/c/apple/datacenters

Bria, F. (2015). *Public Policies for Digital Sovereignty*. Nesta. http://www.nesta.org.uk/report/public-policies-for-digital-sovereignty

Brynjolfsson, E., McAfee, A. (2017). *Machine, Platform, Crowd: Harnessing Our Digital Future*. W.W. Norton & Company.

Canalys. (2025). www.canalys.com/newsroom/europe-smartphone-market-q4-2024

China Telecom. (2025). www.ctamericas.com/global-data-center-map

Cong, W., Thumfart, J. (2022). A Chinese precursor to the digital sovereignty debate: Digital anti-colonialism and authoritarianism from the post-Cold War era to the Tunis Agenda. *Global Studies Quarterly*, 2(4) https://doi.org/10.1093/isagsq/ksac059

Creemers, R. (2020). *China's Approach to Cyber Sovereignty*. Berlin: Konrad Adenauer Stiftung.

Danielsson, J., Macrae, R., Uthemann, A. (2025). Artificial intelligence and financial stability: A systemic risk approach. In: Andrae, S. (ed.), *Economic and political implications of AI* (pp. 23–45). IGI Global.

Data Center Map. (2025). www.datacentermap.com/datacenters

DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

Dykas, P., Koscielniak, P., Tokarski, T. (2013). Taxonomic indicators of economic development of provinces and counties. In: M. Trojak, T. Tokarski (eds.), *Statistical analysis of spatial economic and social differentiation of Poland* (pp. 81–110). Jagiellonian University Publishing House.

European Central Bank. (2025). data.ecb.europa.eu

European Commission. (2023). *Digital Economy and Society Index (DESI) 2023*. https://digital-strategy.ec.europa.eu/en/policies/desi

European Council. (2021). *Speech by President Charles Michel at the DIGITALEUROPE "Masters of Digital" event*. www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event

Fernandez, J. (2025). *The leading generative AI companies*, IOT-analytics, https://iot-analytics.com/leading-generative-ai-companies

Fratini, S., Hine, E., Novelli, C., Roberts, H., Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society*, 3(3), 59. https://doi.org/10.1007/s44206-024-00146-7

George, A.S. (2024). When trust fails: Examining systemic risk in the digital economy from the 2024 CrowdStrike outage. *Partners Universal Multidisciplinary Research Journal*, 1(2), 134–152. https://doi.org/10.5281/zenodo.12828222

Glasze, G., Cattaruzza, A., Douzet, F., & Pauli, A. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, 28(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070

Google. (2025). datacenters.google/locations

Hollo, D., Kremer, M., & Lo Duca, M. (2012). *CISS – A composite indicator of systemic stress in the financial system*. European Central Bank, Working Paper Series No. 1426.

IMF. (2024). *Global Financial Stability Report – Artificial Intelligence and Systemic Risk*.

Madiega, T. (2020). *Digital sovereignty for Europe (Briefing PE 651.992)*. European Parliamentary Research Service. www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651992

Meta. (2025). datacenters.atmeta.com

Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? *Journal of European Public Policy*, 31(8), 2200–2225. https://doi.org/10.1080/13501763.2024.2318475

Musiani, F. (2013). Network architecture as internet governance. *Internet Policy Review*, 2(4). https://doi.org/10.14763/2013.4.208

OECD GPAI (2025), VC investments in AI by country, https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=vc-investments-in-ai-by-country

Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. *Journal of Cloud Computing: Advances, Systems and Applications*, 5(4), 1–18. https://doi.org/10.1186/s13677-016-0054-z

Oxford Insights. (2023). *Government AI Readiness Index 2023*.

PEI. (2025). *Europe needs more investments in cybersecurity, Polish Economic Institute*, https://pie.net.pl/en/europe-needs-more-investments-in-cybersecurity

Pohle, J., Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1532

Pohle, J., Nanni, R., Santaniello, M. (2025). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet*, 16(4), 666–671. https://doi.org/10.1002/poi3.437

Soetan, T. (2023). Challenges in the adoption of AI-powered business intelligence dashboards across sectors. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol 9(4), pp. 524–536.

Srivastava, S., Bullock, J. (2024). AI, global governance, and digital sovereignty. *Global Governance Institute Working Paper* 24–06. https://doi.org/10.48550/arXiv.2410.17481

Statista. (2025), www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers

Tencent. (2025). www.datacentermap.com/c/tencent-cloud

Thumfart, J. (2022). The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the COVID crisis 2020/21 as catalytic event. In: D. Hallinan, R. Leenes & P. de Hert (eds.), *Data Protection and Privacy: Enforcing Rights in a Changing World* (pp. 3–24). Hart. https://doi.org/10.5040/9781509954544.ch-001

Voronoi. (2025), www.voronoiapp.com/technology/Ranked-Top-Countries-by-Computing-Power-3188

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.