July 2026

The Rising Risk of Digital Sovereignty Washing

How sovereignty narratives are overtaking corporate reality

Contents

Executive Summary

Digital sovereignty is rapidly becoming one of Europe's defining corporate narratives. Boards discuss it, governments promote it, and customers increasingly expect it. Yet many organizations are finding that talking about sovereignty is easier than consistently demonstrating it. That gap matters. As stakeholder expectations rise and definitions remain fluid, a new category of reputational risk — and increasingly one that may attract regulatory scrutiny — is emerging: digital sovereignty washing — the promotion of digitally sovereign operations, products, or capabilities that external audiences perceive as not or only partially realized.

Kekst CNC analyzed 233 public communications from 60 large European companies across sectors where sovereignty is a key or emerging consideration, including technology and telecommunications, defense, finance and healthcare.

Three patterns stand out:

1. **Communications are accelerating faster than proof.** Sovereignty messaging has risen, yet only 64% of analyzed communications include a clear, directly supporting proof point. The gap varies significantly by sector, with technology leading (69%), followed by finance and healthcare (60% each), and defense (51%).

2. **Companies prove what they are selling more often than how they operate.** Where supporting evidence exists, 81% relates to products, partnerships, or customer offerings rather than internal governance, infrastructure, or operational controls.

3. **The language remains unsettled. There is no shared definition.** "Digital sovereignty" is the umbrella term, but organizations use a range of concepts, including 'strategic autonomy,' 'cloud sovereignty,' 'data sovereignty,' 'European industrial capacity,' 'compliance,' and the emerging theme of 'AI sovereignty.'

For communications and corporate affairs leaders, the implication is clear:
The next phase of the digital sovereignty debate will not be won through messaging alone. Credibility depends on the ability to demonstrate, rather than simply declare, sovereign capability.

Context

Europe has spent much of the past decade debating who should control its data, digital infrastructure, and critical technologies. Regulatory milestones accelerated that discussion. More recently, geopolitical tensions have transformed dependency risks from legal abstractions into tangible operational concerns.

Stakeholder expectations have shifted just as quickly. Mentions of digital sovereignty and related concepts in English-language top-tier media increased by almost 50% in the twelve months to April 2026 compared with the previous year. As sovereignty frameworks become more standardised, claims are also becoming more testable in practice (e.g., EU's CADA sovereignty assurance framework).

As stakeholders have started asking sharper questions, companies have begun to differentiate themselves along various lines. Several positioning archetypes are now visible in the market:

Figure 1. Emerging archetypes of digital sovereignty positioning

Sovereign Champions:
Primarily European telecoms and technology companies positioning ownership, operations and values as a competitive alternative to non-European providers.

Risk-focused Compliers:
Companies that present sovereignty primarily as a risk-management and governance issue rather than a commercial opportunity.

Product Accommodators:
Largely U.S. hyperscalers (e.g., AWS and Microsoft) treating digital sovereignty as a distinct offering for European buyers.

Strategic Autonomy Advocates:
Defence, aerospace and critical-infrastructure companies extending long-standing strategic-autonomy narratives into the digital domain.

The Silent Rest:
Industries such as oil and gas, or consumer goods, where sovereignty remains peripheral to the core corporate narrative — with some exceptions.

AI Sovereignty Evangelists:
A newer group framing sovereign AI capabilities as the next frontier for digital independence.

To understand how companies are positioning themselves — and where the gap between narrative and operational reality is widest — Kekst CNC analyzed communications from 60 large European companies across technology and telecommunications, defense, finance, and healthcare.

Of the 233 communications reviewed, 197 met the threshold for explicit digital sovereignty positioning and form the basis of this analysis.

Three Communications Takeaways

1. Communications are accelerating faster than proof points.

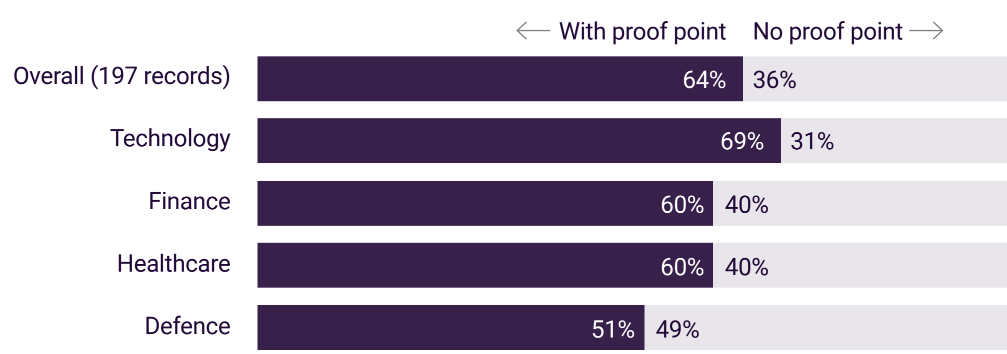
The conversation around digital sovereignty communication has expanded rapidly, but evidence underpinning it has not always kept pace.

Across the 60 companies analyzed, communications explicitly focused on digital sovereignty rose more than sixfold between the pre-2024 period and 2024–2026. The inflection coincides with Europe's strategic autonomy push and the political response to a shifting geopolitical landscape.

Yet only 64% of the 197 communications included in the core data set contain a clear supporting implementation or proof point. Put differently, about one in three sovereignty claims could be perceived as marketing without sufficient evidence being provided directly.

The gap also varies by sector. Technology companies show the highest level of substantiation (69%), while others rely more heavily on broad language with comparatively fewer concrete examples.

Figure 2. Share of counted sovereignty communications directly backed by a clear proof point



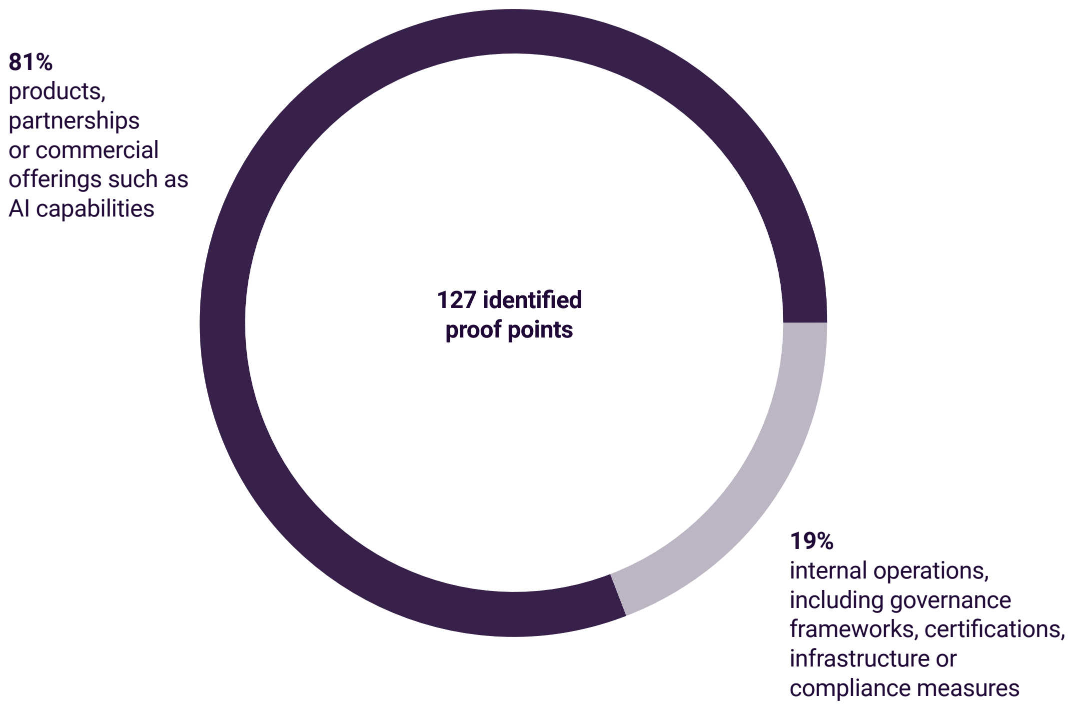
2. Companies prove what they sell more often than how they operate.

When organizations support sovereignty claims with evidence, that evidence is overwhelmingly customer-facing.

Of the identified proof points, 81% relate to products, partnerships, or commercial offerings, such as AI capabilities. Only 19% relate to internal operations, including governance frameworks, certifications, infrastructure, or compliance measures.

The findings also highlight an underlying market tension. Several companies explicitly reference a U.S. hyperscaler alongside sovereignty claims. This does not amount to sovereignty washing, but it creates a complexity that external stakeholders may increasingly scrutinize. It also reflects a market reality — U.S. hyperscalers continue to account for roughly 70% of the European cloud market.

Figure 3. Examples of what proof points companies cite as evidence.



KEKST CNC

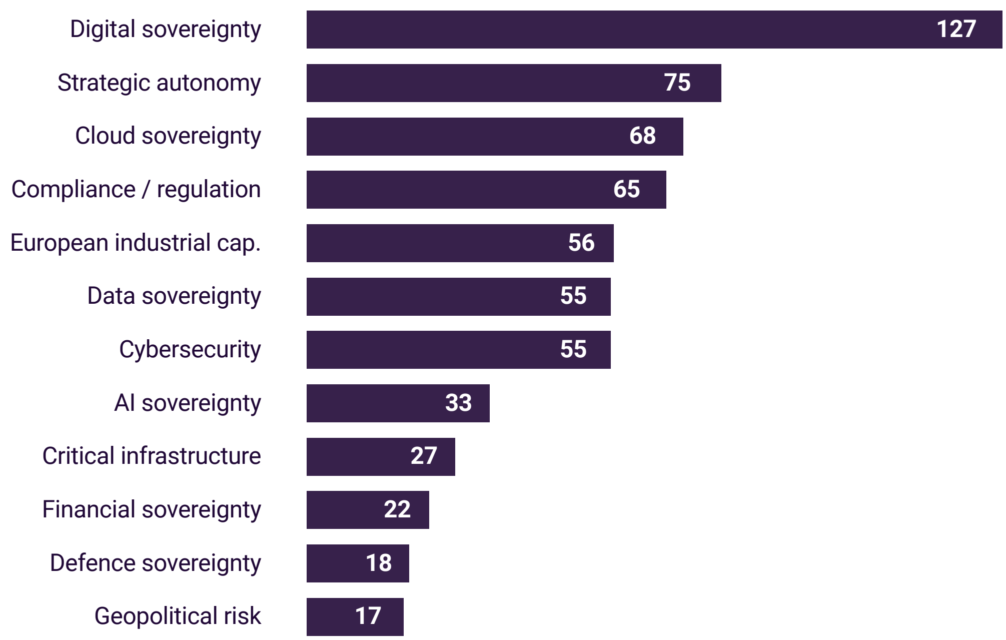
3. The language remains unsettled.

Digital sovereignty is becoming a widely used concept, but not yet a consistently defined one.

The dataset captured at least several closely related terms used to describe similar ideas. “Digital sovereignty” remains the dominant phrase, alongside “strategic autonomy,” “cloud sovereignty,” “compliance/regulation,” “European industrial capacity,” “cybersecurity,” “data sovereignty,” and the emerging concept of “AI sovereignty.”

These terms often appear together and are frequently used interchangeably. The absence of a settled vocabulary creates room for both genuine ambiguity and strategic flexibility. The rapid rise of the term “AI sovereignty”, largely a recent phenomenon, indicates where the debate is heading. This diversity of terms makes it harder for stakeholders to assess sovereignty claims, especially as expectations become more defined.

Figure 4. Most frequently used vocabulary used by companies when speaking about digital sovereignty



Implications: What Communications Leaders Should Do Next

Digital sovereignty is evolving into a distinct category of reputation risk. As stakeholder expectations rise and definitions remain fluid, the organizations that succeed will be those that can match narrative with demonstrable action. Those that cannot may find broad claims increasingly being assessed against emerging procurement criteria and externally verifiable standards, with any perceived gaps triggering commercial consequences.

Principles for navigating the tension:

Create clarity on sovereignty readiness: Start with an honest internal assessment — how sovereign is the organization right now, where are the vulnerabilities, and what is the strategic ambition? Then clearly map and understand how your stakeholders would perceive different sovereignty claims. Decide whether sovereignty is a market-shaping ambition, a customer requirement, or a compliance baseline. Each position carries different trade-offs and demands different forms of evidence.

Be precise about your definition. Without a unified definition, clearly framing what is meant by sovereignty in the company's context is key. Then be clear about the level of control. Different layers, e.g. data residency, jurisdictional control, or operational autonomy, are different commitments. Each has different implications and defensibility.

Lead with evidence, not marketing. The most credible organizations anchor their sovereignty claims in something verifiable. These are the details journalists, regulators, and investors are most likely to test. At the same time, sovereignty will more often than not be a journey. Progress, not perfection, is often the more credible story.

Methodology

Kekst CNC analyzed 233 communications records published until April 2026 (the majority from 2024–2026) by 60 large European companies across technology and telecommunications, defense, finance, and healthcare. The dataset draws on companies' public-facing communications: press releases, annual reports, blog posts, owned web content, earnings presentations, and articles.

Data collection followed three stages. First, AI-assisted research identified companies explicitly referencing digital sovereignty or closely related concepts, with results validated by human review. Second, a base dataset of sovereignty-related claims and proof points was compiled. Third, Kekst CNC analysts conducted a detailed manual review, verifying records against original sources, refining and supplementing the dataset, classifying entries by source, theme, and proof-point typology, and assessing whether language met the threshold for explicit sovereignty positioning. Records that did not meet this threshold were retained but excluded from frequency counts. The curated dataset was then analyzed quantitatively, combining AI support with human sense-checking.

The analysis has three key limitations:

First, the sample of 60 European companies is selective, covering key sectors and geographies, but is not fully representative.

Second, theme and proof-point classifications reflect how companies communicate sovereignty, not necessarily underlying operations.

Third, certain flags (e.g. hyperscaler dependency, certification, European vendor) indicate lack of reference in the communications, not absence of the underlying fact.

Kekst CNC is the international strategic communications advisory firm within Publicis Groupe. For more than 50 years, companies and institutions have turned to Kekst CNC in moments that define reputation. With offices in the world's leading corporate and financial centers, the firm combines insight, creativity and sound judgment to partner with clients seeking to grow, transform and protect their organizations.

Reach out to Kekst CNC's contested situations experts:

Dominic Reynolds
Partner
Dominic.Reynolds@kekstcnc.com

Sean Evins
Partner
Sean.Evins@kekstcnc.com

Mikey Hoare
Partner
Michael.Hoare@kekstcnc.com

Laura Grünberg
Director
Laura.Gruenberg@kekstcnc.com