Policy Brief 2026

Cloud and AI Development Act (CADA): From regulatory ambition to European industrial capacity



Telefónica

Telefónica

Index

1. **Executive summary**

2. **What is at stake in CADA**

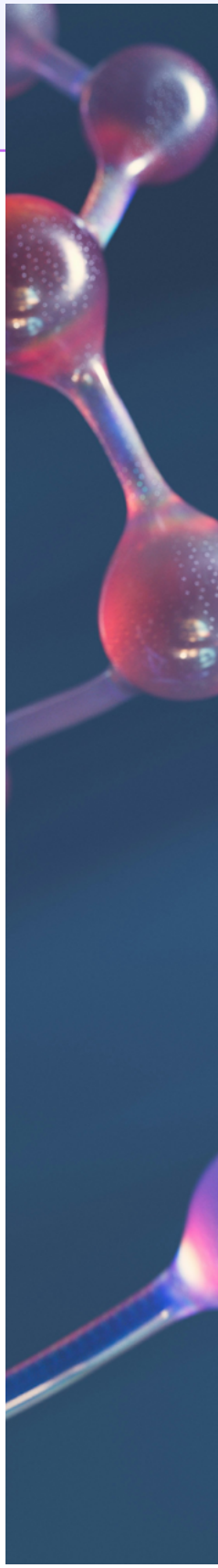
3. **Making CADA work**

4. **Operators and digital services:** a European industrial platform

5. **Recommendations**

* **References**

1. Executive summary



Europe aims to reduce its technological dependence in cloud computing and artificial intelligence (AI), the two infrastructures that will underpin much of the economy over the next decade. The starting point is challenging: European providers account for around 15% of the European cloud infrastructure market, down from 29% in 2017, while three major US providers hold close to 70%[1]. The Cloud and AI Development Act (CADA), proposed by the European Commission on 3 June 2026[2], is the legislative response: it aims to triple European data centre capacity within five to seven years[3], using public procurement to foster a trusted European offering. Its strategic value will depend on whether these measures translate into new services, more providers and genuine alternatives for businesses and public authorities.

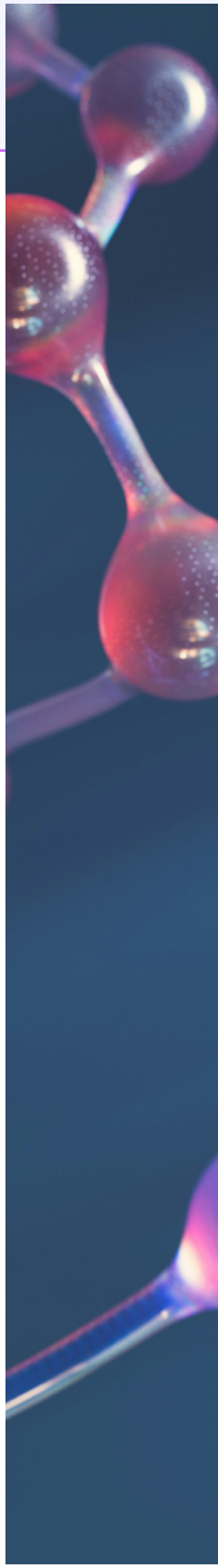
Telefónica supports CADA's ambition. Its priority is for the Regulation to mobilise private investment, strengthen European industrial capacity and maintain openness to trusted technology partners, always subject to verifiable conditions of control. The risk to avoid is a paradoxical one: high compliance costs, poorly defined exemptions or twenty-seven different national approaches to implementation could inadvertently strengthen the position of those already dominating the market.

This paper applies to cloud and AI the vision set out in Telefónica's Policy Brief "European technological sovereignty: connectivity, investment and scale for a Europe with the capacity to choose"[4]. It does not repeat that brief's geopolitical analysis: it focuses on the regulatory decisions that would turn Europe's connectivity and distributed infrastructure into a competitive digital services offering.

CADA's success should be measured by the capacity actually deployed, investment mobilised, provider diversity, reduced external dependencies and actual service uptake. To achieve this, Telefónica sets out five priorities combining industrial ambition, verifiable sovereignty and workable rules:

- Effective and verifiable sovereignty levels. Genuine European control, demonstrated against common criteria.
- Edge cloud: turning Europe's extensive infrastructure footprint into a competitive advantage. Support for distributed infrastructure deployment.
- Recognition of existing certifications. Reuse of safeguards already certified.
- Public procurement supporting industrial policy and sovereignty. Public demand to foster European solutions.
- A targeted and proportionate potential extension to the private sector. Application limited to demonstrated material risks.

2. What is at stake in CADA

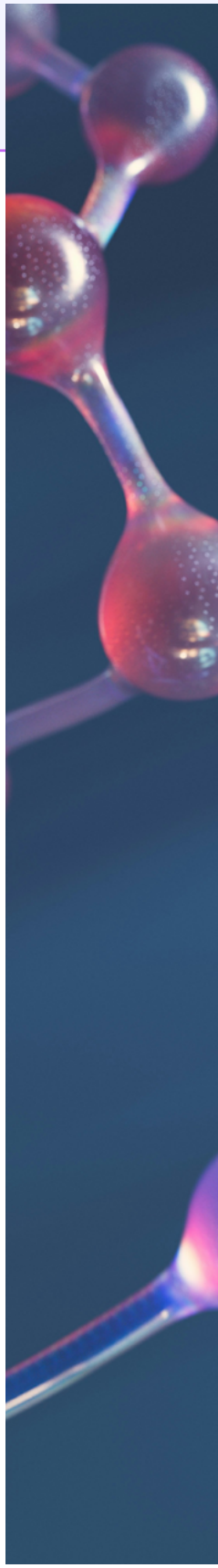


CADA combines supply-side measures, enabling more data centres to be authorised faster, with demand-side measures governing which cloud and AI services the public sector may procure. For Telefónica, what matters is how these instruments work together: project acceleration, assurance levels, public procurement and open source must jointly create a viable and competitive European market for cloud and AI services. Its four main components are:

- Sovereignty framework. Four Union assurance levels, with progressively more stringent requirements, for cloud and AI services procured by the public sector. All services must meet the first level; following a risk assessment, the higher levels will apply to the most sensitive services, likely including those relating to energy, transport, healthcare, banking, national security, borders, public order or defence.
- Union added value. In public procurement of cloud and AI services, public authorities will also assess each bid's contribution to European industrial capacity. This will be a complementary criterion: it adds points but does not determine the award on its own[5].
- Accelerating data centre deployment. At least one acceleration zone per Member State, with consolidated permitting and a maximum timeframe of 12 months for project authorisation, alongside strategic projects with preferential access to European funding.
- Open source first. The public sector must prioritise open-source software, supported by a European catalogue of solutions. The European Open Source Strategy accompanying CADA estimates that the EU spends around €264 billion a year on US proprietary IT products and services[6].

Its effectiveness will depend on verifiable criteria, harmonised implementation across Member States and a clear relationship with NIS2[7], cybersecurity certification and public procurement rules. Preserving the capacity to innovate and preventing exemptions from undermining the industrial objectives will be equally important.

3. Making CADA work



The following five priorities translate Telefónica's position into concrete policy decisions. The aim is for CADA to strengthen European capabilities, attract investment and provide genuine alternatives, with clear, proportionate and verifiable requirements.

Effective and verifiable sovereignty levels

Assurance levels must measure genuine control, going beyond the provider's place of establishment or the location of the data. Each level must represent a clear and verifiable improvement in Europe's capacity to make decisions, operate and maintain the service. The assessment must cover who makes critical decisions, manages privileged access and keys, maintains and updates the technology, ensures continuity and can replace essential components.

CADA should establish a harmonised and auditable framework across all Member States. Level 1 must include robust baseline safeguards, including encryption and, where justified by risk, independent key management. Level 2 must recognise partnerships in which a European entity has the authority and capability to take responsibility for operations, security and continuity. Level 3 must require verifiable European control over critical operations. Level 4 must be reserved for the most sensitive uses and demonstrate the autonomous capacity to maintain, update, further develop and replace essential components.

International technologies and partnerships must remain possible where the European partner retains such effective control. Corporate structures, contracts, exemptions or agreements with third countries should not allow a service to qualify for a high assurance level if an external entity or authority can access data, block updates, degrade the service or prevent its continuity in Europe.

Edge cloud: turning Europe's extensive infrastructure footprint into a competitive advantage

Europe can complement large data centres with distributed capacity close to factories, hospitals, ports, cities and public services. This proximity improves latency, resilience and control over data, enabling the benefits of cloud and AI to extend beyond the major technology hubs.

CADA must therefore ensure that distributed architectures are included in the measures covering acceleration zones, permitting, administrative coordination, access to the electricity grid and certification, applying criteria that are neutral as regards technology, size and location. It must also recognise telecommunications operators as strategic enablers, given their extensive infrastructure footprint, connectivity, territorial reach and expertise in security and continuity.

Funding and incentives must facilitate the conversion of existing communications sites into secure and resilient computing capacity. Open standards, interoperability and portability must enable nodes to be federated and prevent new dependencies between cloud and edge environments.

Recognising certifications to move faster

Europe must build on controls already assessed under rigorous national schemes. Telefónica proposes establishing an official mapping between comparable national certifications and CADA's assurance levels across all Member States. Equivalent controls should be recognised automatically, with any additional assessment focused on the remaining gaps: effective European control, personnel location and access, jurisdictional exposure, the use of data for AI training and transparency in the software supply chain.

Providers with valid supporting evidence should receive provisional accreditation while completing this targeted assessment. This equivalence-based approach must apply to comparable national schemes, avoiding duplicate audits, unnecessary costs and competitive disadvantages.

For example, in Spain, the High category of the National Security Scheme (ENS Alto) covers a substantial share of the technical, organisational, continuity and audit safeguards, although it does not by itself certify all aspects of sovereignty and control. In this case, Telefónica proposes that CCN-CERT and ENISA establish an official mapping between ENS Alto and level 3.

Public procurement supporting industrial policy and sovereignty

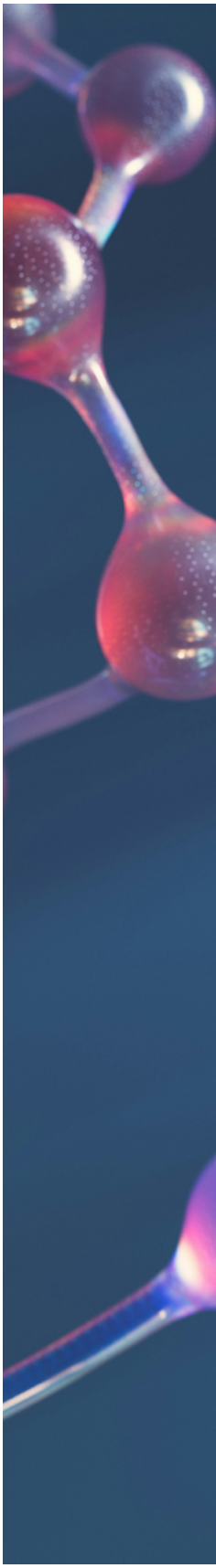
Public authorities can act as anchor customers for European cloud, edge, cybersecurity and AI solutions. Within its sectoral scope, CADA must introduce public procurement criteria covering security, resilience, innovation, continuity, operational control, jurisdictional exposure, data and key management, and contributions to European value chains, complementing horizontal legislation without duplicating it.

Requirements must be proportionate to the criticality of the service and offer a genuine opportunity to European operators and specialist providers. Global scale or an established market position cannot serve as substitutes for quality, security or resilience. Well-targeted public demand can reduce investment risk, build reference projects and help more providers compete in the single market.

The exemptions under Article 30(4) must be genuinely exceptional, justified and transparent. Otherwise, their widespread use by contracting authorities could undermine the purpose of these provisions and compromise CADA's effective implementation. In particular, the exemption on grounds of disproportionate cost must be narrowly defined through restrictive, objective and verifiable criteria to prevent it from hollowing out sovereignty requirements or entrenching the providers with the greatest market power.

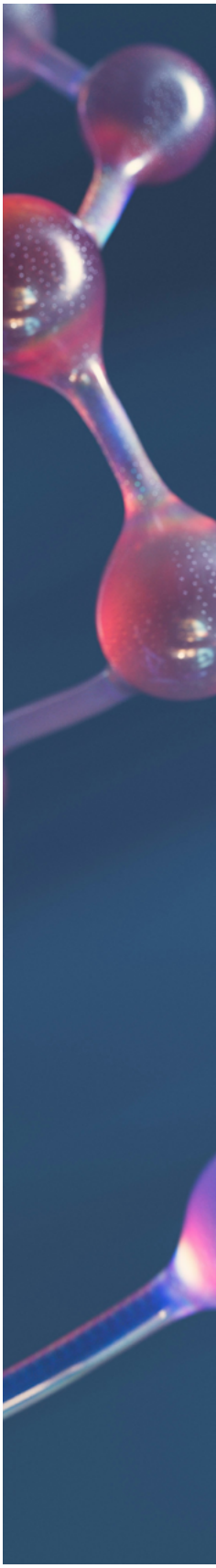
A targeted and proportionate extension to the private sector

Companies providing services critical to the economy and society and falling within the scope of the NIS2 cybersecurity Directive must not be arbitrarily subjected to new sovereignty obligations concerning the cloud and AI services they use. The specific circumstances that could justify extending CADA's obligations to the private sector, the public interest grounds underpinning such an extension and the objective criteria determining its scope and the extent of the requirements imposed must be defined in advance. Article 31 should thus operate as a safeguard limited to third-party cloud or AI services presenting material and demonstrated sovereignty risks that existing frameworks cannot address.

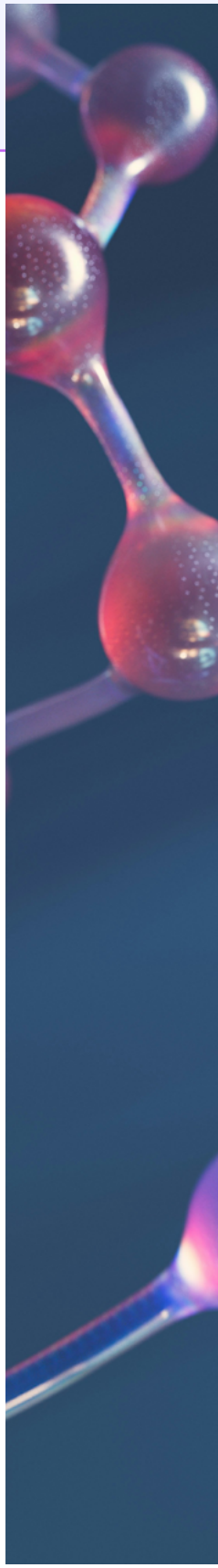


Requirements must be proportionate to the sensitivity of the service and its importance to critical operations, taking into account exposure to third-country laws and authorities, effective operational control and the availability of credible European alternatives. Where intervention is justified, affected companies must be given realistic and sufficient transition periods to adapt their systems, contracts and migration plans, without disrupting critical operations or delaying network transformation. CADA must clearly distinguish those services from cloud-native network functions deployed and managed by operators on their own infrastructure, which are already subject to sector-specific security and resilience requirements.

Before adopting any delegated act, the Commission must conduct a sectoral impact assessment, publish the evidence, consult affected companies, associations, providers, operators, experts, authorities, regulators, ENISA and users, and explain how their input has been incorporated. Any intervention must precisely define its scope, objectives, transition arrangements and review process, reusing existing controls and avoiding duplicate audits, reporting and certifications.



4. Operators and digital services: a European industrial platform

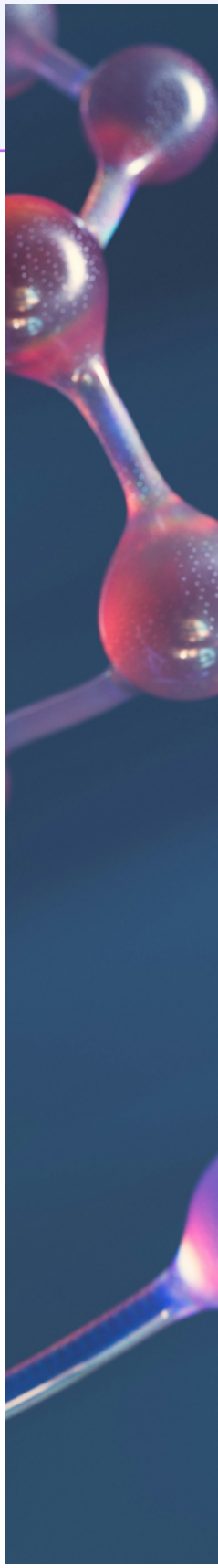


Operators can bring much more than connectivity to CADA: distributed sites, network and security capabilities, data centres, their own cloud services and direct relationships with industrial and public-sector customers. According to Connect Europe, in 2025 they owned around 19% of European data centres and had deployed some 750 edge nodes by the end of 2024[8]. This combination of local and centralised capacity enables the deployment of AI services with differing latency, resilience and control requirements.

The federation of edge infrastructure, such as the pan-European edge continuum launched by Deutsche Telekom, Orange, Telefónica, TIM and Vodafone at MWC 2026[9], together with open standards and portability, can expand Europe's offering beyond the major computing hubs. To turn this potential into a market, CADA must recognise operators as providers and integrators of digital services, with access to strategic projects and support mechanisms on transparent terms.

The investment needed to develop cloud, edge and AI far exceeds what public funding can provide: European policy must create the conditions to mobilise private capital and sustained demand. The broader debate on the single market for networks, competition and scale is addressed in the Policy Brief on technological sovereignty[10]; here, the specific priority is for CADA to enable European cloud and edge services to become commercially viable and scale up.

5. Recommendations



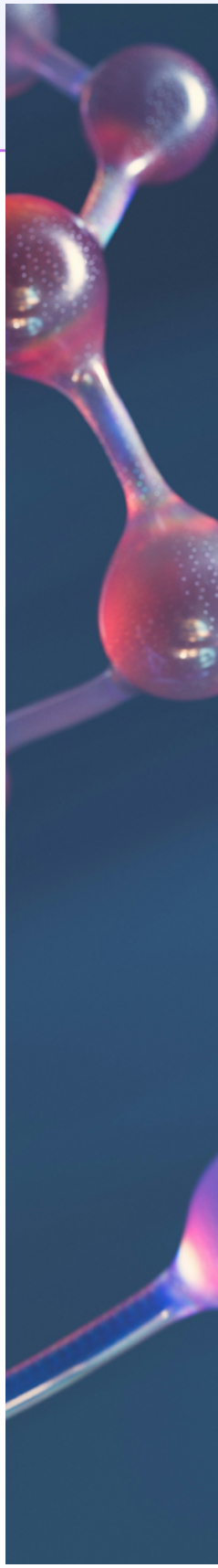
Telefónica proposes focusing the CADA negotiations on decisions that make a tangible difference to market capacity:

- Define effective and verifiable sovereignty levels, with a common European framework covering decision-making, access, keys, jurisdiction, continuity, dependencies and substitutability; require a genuine increase in control at each level and allow international partnerships only where European control can be demonstrated.
- Turn edge cloud into a European competitive advantage, including distributed infrastructure in permitting, acceleration zones, funding, certification, connectivity and electricity access measures; recognise the role of operators and promote federation, interoperability, portability and open standards.
- Recognise rigorous national certifications, through an official mapping between ENS Alto and level 3, automatic reuse of equivalent controls, additional assessment limited to sovereignty gaps and provisional accreditation; extend this approach to comparable schemes in other Member States.
- Use public procurement to support industrial policy and sovereignty, taking account of security, resilience, innovation, continuity, operational control and European contribution; ensure genuine opportunities for a diverse range of providers and limit the exemptions under Article 30(4) through objective, transparent and verifiable criteria.
- Ensure that any extension to the private sector is targeted and proportionate, limited to material risks in third-party services, without automatic application on the basis of NIS2; distinguish cloud-native network functions, require an impact assessment and sectoral consultation, and provide for a defined scope, transition arrangements, review and the avoidance of duplication.

CADA can become a decisive component of European digital industrial policy if it turns regulatory ambition into infrastructure, competitive services and genuine demand. To do so, it must recognise the value of edge computing, substantiate sovereignty through evidence of effective control and enable European providers, including operators, to invest and scale up.

CADA's success must be measured not only by the infrastructure deployed, but also by its contribution to Europe's autonomy in operating, maintaining and further developing cloud services, ensuring their continuity and the capacity to decide on their future development. Cooperation with trusted international technology partners is compatible with this objective and must reinforce it, on the basis of risk-proportionate requirements whose implementation can be verified, although delivery in the market will depend to a large extent on legal certainty and public procurement.

* References



1. Synergy Research Group, "European Cloud Providers' Local Market Share Now Holds Steady at 15%", 24 July 2025: https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15. See also Copenha¬gen Economics, Cloud sector brief, June 2026: https://copenhageneconomics.com/wp-content/uploads/2026/06/Copenhagen-Economics_Cloud-sector-Brief.pdf

2. European Commission, Proposal for a Regulation on cloud and artificial intelligence development (Cloud and AI Development Act), COM(2026) 502, 3 June 2026.

3. Ibid. The objective was initially set out in European Commission, AI Continent Action Plan, COM(2025) 165, 9 April 2025.

4. Telefónica, Policy Brief "European technological sovereignty: connectivity, investment and scale for a Europe with the capacity to choose", November 2026.

5. According to the recitals of the proposal, the criterion should be "ancillary and non-decisive", with an indicative maximum weighting of 15 out of 120 points. European Commission, COM(2026) 502, cited above.

6. European Commission, European Open Source Strategy, 3 June 2026. For an analysis of the package, see Covington, "The EU Cloud and AI Development Act in Depth", Global Policy Watch, June 2026: https://globalpolicywatch.com/2026/06/the-eu-cloud-and-ai-development-act-in-depth

7. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), OJ L 333, 27.12.2022.

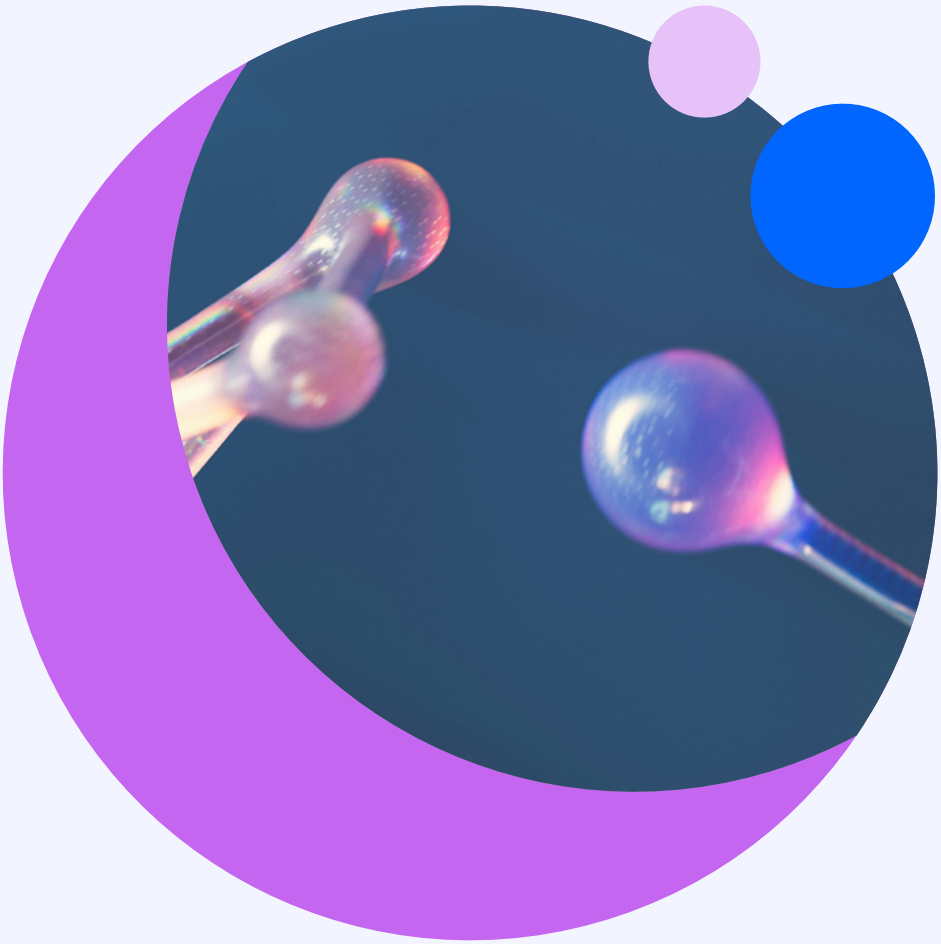
8. Connect Europe, State of Digital Communications 2026, February 2026: https://connecteurope.org/insights/reports/state-digital-communications-2026.

9. Telefónica, "Deutsche Telekom, Orange, Telefónica, TIM and Vodafone achieve the first federated pan-European Edge Continuum at MWC 2026", press release, February 2026: https://www.telefonica.com/es/sala-comunicacion/prensa/deutsche-telekom-orange-telefonica-tim-vodafone-logran-primer-edge-continuum-federado-paneuropeo-mwc-2026/

10. Telefónica, Policy Brief "European technological sovereignty...", cited above.

Policy Brief
2026

Cloud and AI Development Act (CADA): From regulatory ambition to European industrial capacity



Follow the conversation on:
our Web, LinkedIn o subscribe to our Newsletter

Telefónica

Public Policy, Regulation and Competition