Spanish decree on network security and resilience

Spain has published a Royal Decree on the security and resilience of electronic communications networks and related digital infrastructure. While the proposal is primarily rooted in telecommunications and digital connectivity policy, it has direct and growing relevance for the fire safety and security industry, particularly in relation to data centres and critical digital infrastructure. This initiative reflects a broader European trend: network availability, operational continuity and physical protection are increasingly treated as elements of national resilience, alongside cybersecurity.

A new regulatory focus on network resilience

The proposed decree aims to strengthen the security, robustness and continuity of electronic communications networks and services in Spain. It introduces enhanced obligations for operators of:

- Public electronic communications networks and services
- Supporting digital infrastructure, including data centres, internet exchange points and other critical facilities

The objective is to ensure that these infrastructures remain operational during incidents, including cyber events, physical disruptions, power failures and emergencies.

While the decree is distinct from the EU NIS2 Directive, it clearly aligns with the same policy logic: essential digital services must be resilient, well-protected and rapidly recoverable.

Explicit relevance for data centres

One of the most significant elements of the draft decree is the explicit inclusion of data centres that support electronic communications networks and services, subject to defined thresholds. For data centre operators, this translates into obligations to:

- Develop documented security and resilience plans
- Address risks related to physical infrastructure, power supply and continuity
- Implement procedures for incident detection, escalation and reporting

- Demonstrate preparedness for service disruptions affecting network availability

This approach recognises that data centres are no longer neutral technical facilities, but critical nodes in national digital infrastructure.

Importance for the fire safety and security industry

Although the decree does not explicitly regulate fire safety or security products, its requirements cannot be met without robust physical protection systems. This creates a clear and strategic role for the fire safety and security sector.

Fire risk as a resilience issue

For data centres and network infrastructure, fire is among the highest-impact risks, capable of causing prolonged service outages with national or regional consequences. The decree implicitly elevates fire prevention, detection and suppression from a building-level concern to a network resilience priority.

Physical security supports continuity

The protection of critical installations includes:

- Controlled access to sensitive areas
- Intrusion detection and perimeter protection
- Monitoring of critical nodes

These measures directly support the decree's objective of maintaining availability and integrity of network services.

Incident detection and reporting

The decree introduces very short incident notification timelines. Fire and security systems are often the first source of alerts, making their reliability, accuracy and integration essential for compliance.

From Compliance to Supply-Chain Expectations

Even where fire safety and security companies are not directly regulated entities, they form part of the compliance ecosystem of data centres and network operators.

Customers are therefore likely to demand:

- High system reliability and redundancy
- Secure connectivity and cyber-resilient components
- Clear documentation and lifecycle management
- Alignment with relevant European and international standards

This mirrors developments under NIS2, where regulatory expectations increasingly extend into the supply chain.

Strategic opportunity

The Spanish decree illustrates a wider shift in European policy thinking: physical safety, security and cybersecurity are converging under the concept of resilience. For the fire safety and security industry, this represents an opportunity to:

- Position fire detection and suppression as essential resilience measures
- Demonstrate how physical protection contributes to network availability
- Engage policymakers to ensure that fire risks are properly recognised in digital infrastructure regulation
- Support customers in meeting new resilience and continuity obligations

Looking Ahead

The direction of the Royal Decree is clear: digital resilience depends on physical resilience. For Euralarm members active in fire safety, security systems, system integration or services for data centres and critical infrastructure, this is a development worth close attention — and proactive engagement.

www.euralarm.org