Digital Networks Act

2026/0013(COD) - 21/01/2026 - Legislative proposal

PURPOSE: to create a new Digital Networks Act (DNA) to modernise, simplify and harmonise EU rules on connectivity networks.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: technologies are rapidly evolving, data traffic is growing significantly, and demand for gigabit connectivity is increasing. Modern and sustainable digital infrastructures for connectivity and computing are critical enablers for digitalisation and therefore both for the industrial competitiveness and for society to benefit fully from digital services. For that reason, high-quality, secure and resilient connectivity for everybody and everywhere in the Union is needed. The internal market in the area of electronic communications remains fragmented into 27 national markets and European operators continue to face barriers to operating cross-border and scaling-up, limiting their ability to invest, innovate, and compete in the extended connectivity ecosystem on a level-playing field.

This proposed Regulation repeals Regulation (EU) 2018/1971 establishing the Body of European Regulators for Electronic Communications (BEREC), Directive (EU) 2018/1972 (European Electronic Communications Code) and Decision No 243/2012/EU establishing a multiannual radio spectrum policy programme, and amends existing legislation on open internet access, electronic communications privacy and spectrum policy.

By **replacing directives with a regulation**, it ensures uniform application across all Member States.

The Act forms part of the EU’s broader digital and industrial policy objectives, including digital sovereignty and strategic autonomy.

CONTENT: the Digital Networks Act establishes a **new EU framework for digital connectivity networks** in order to support the development of high-performance, secure and resilient digital infrastructures across the Union. It responds to growing connectivity needs driven by digitalisation, emerging technologies and strategic autonomy considerations.

Transition to advanced connectivity networks

Legacy copper networks do not fit the ambition of making innovative technologies widely available across the EU. The DNA introduces mandatory national transition plans to ensure the phase out of copper networks and the transition to advanced networks between 2030 and 2035. Member States must present their national plans in 2029. These national plans will explain (i) in which areas copper will be switched off and by when and (ii) the measures to support the transition to fibre. In the initial phase, Member States will be required to mandate the copper-switch-off in areas where the following two conditions are cumulatively met: (i) at least 95% of fibre coverage and (ii) availability of affordable retail connectivity services. In the latter phase, the conditions will no longer play a role and Member States will be required to mandate the switch-off in all the remaining copper switch-off areas except in the areas where fibre deployment is not economically viable and no adequate connectivity solution capable of replacing copper-based services is available. **Safeguards** apply during the entire process in order to maintain continuity and protect consumers.

Simplification and investment

The Digital Networks Act modernises the regulatory framework, reducing administrative burden and reporting obligations, so companies can focus their resources on investment and innovation. The DNA also allows more flexibility for business-to-business relations, while keeping a high level of consumer protection.

Secure and resilient connectivity

The DNA enhances network security and resilience by limiting dependencies in the connectivity ecosystem and promoting EU-level cooperation. The proposal introduces an EU-level Preparedness plan to tackle the rising risks of crises including natural disasters and foreign interference in networks. In addition, the common mechanism for selecting pan-EU satellite communications will incorporate criteria focused on security and resilience.

Protecting net neutrality in innovative services

The DNA fully keeps the principles of net neutrality. It introduces a mechanism to clarify Open Internet rules for innovative services to increase legal certainty and a voluntary ecosystem cooperation mechanism on IP interconnection, traffic efficiency, and other emerging areas. For providers of internet access services, the DNA introduces mandatory **biennial reporting** regarding the safeguarding of net neutrality.

Resilience

The proposal introduces a specific framework for network and service resilience and preparedness, recognising electronic communications networks and services and other digital infrastructures are essential to the functioning of society and the economy. To this end, it establishes obligations and cooperation mechanisms to ensure the availability and capabilities of networks and services in situations of major crisis. This includes the continuity of **emergency communications and public warnings**.

Single passport authorisation

The single passporting framework for electronic communications networks and services is established under a general authorisation regime. It affirms the freedom to provide such networks and services across the EU as long as the common further conditions and obligations laid down in this Regulation are met. It also maintains a **streamlined notification-based system** enabling providers to operate in one, several or all Member States on the basis of a single confirmation by one national regulatory authority.

Resources, spectrum and numbering

The proposal establishes a comprehensive and forward-looking framework for the management, allocation, and use of key electronic communications resources. This includes radio spectrum and numbering resources, recognising their role as strategic public goods essential for connectivity, innovation, security, and the functioning of the single market.