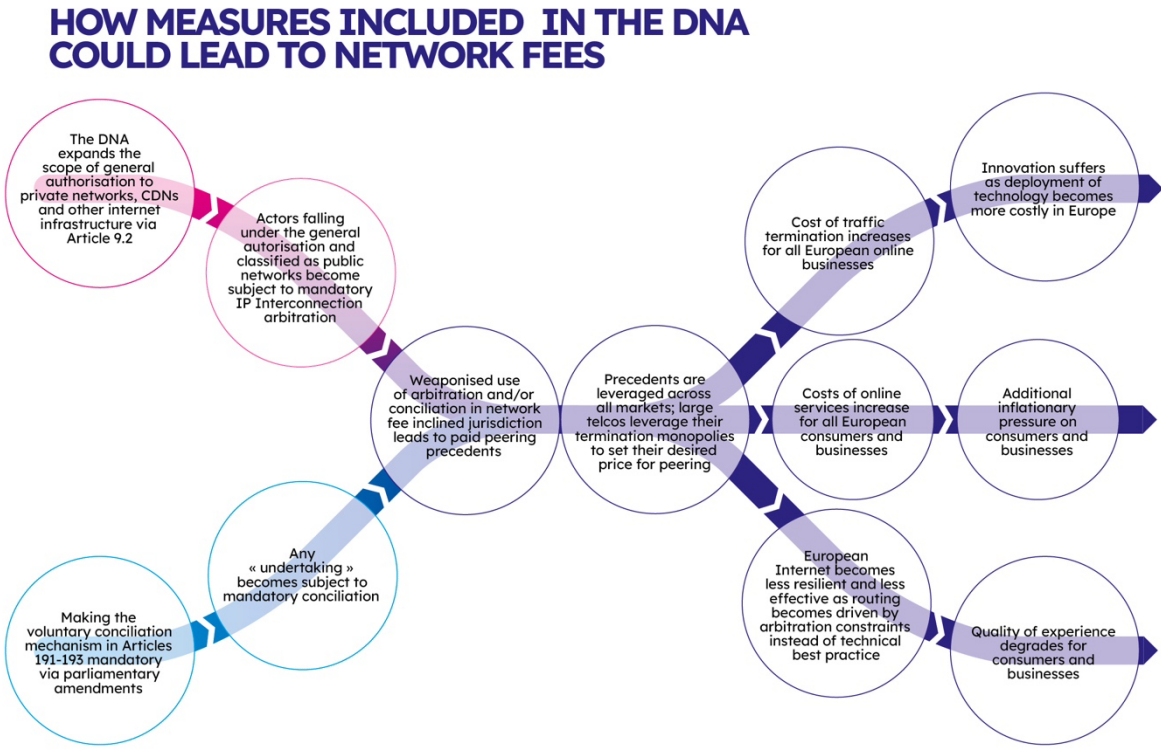
European Commission Legislative proposal for a Digital Networks Act (DNA):

THE DNA RISKS TO IP INTERCONNECTION AND THE BROADER COMMUNICATIONS ECOSYSTEM



Benoit Felten | July 2026

This study is an independent report funded by the Computer & Communications Industry Association (CCIA Europe). The opinions offered herein are purely those of the authors and do not necessarily represent the views of CCIA Europe.

Executive Summary

The European Commission published a legislative proposal for a *Digital Networks Act* (DNA) on 21 January 2026[1]. This text is currently subject to the ongoing co-legislative procedure, involving both the European Parliament and the European Council (Member States). It aims at revisiting, harmonising and simplifying the European framework for telecommunications.

Critically, on IP interconnection[2], the legislation demonstrates an inherent bias about the relationship between telecommunications operators[3] and content and application providers[4] (CAPs), which it considers inefficient.

However, neither the DNA's recitals nor its impact assessment demonstrate such inefficiency. On the contrary, recent studies on the issue show that collaboration between telecom operators and content and application providers is efficient, particularly related to IP Interconnection.

Still, the DNA introduces two distinct measures that pose systemic risks to IP interconnection:

1. The scope expansion of the general authorisation regime to a potentially wide range of actors, including content and application providers, will subject them to increased regulatory burden and to mandated dispute resolution mechanisms (i.e. network fees);
2. The voluntary conciliation mechanism between providers of electronic communications networks and "other undertakings", albeit to a lesser degree than strict network fees. Moreover, if the mechanism becomes mandatory, possibly through a revision clause or during the legislative process, it will lead to the introduction of network fees and make virtually any online business a target for *mandated* conciliation.

The fact that the DNA presents two distinct mechanisms to target content and applications providers with different scopes and different inner workings only compounds the issue, and is firmly at odds with any intent to actually simplify regulation and reach goals of network resilience, or overall competitiveness.

Mandating IP Interconnection agreements and regulating their prices can only have deleterious effects:

- higher costs for transit providers, Content Delivery Networks (CDNs) and private network owners including CAPs' private networks: transit providers and CDN providers are especially likely to be targeted by telecom operators wanting to generate revenue from traffic exchanges.
- higher costs for consumers and European online businesses: higher costs for traffic delivery for CDNs and transit providers will trickle down to their customers, including tens of thousands of small European online businesses that rely on these traffic carriers to meet their customers' demand. Costs of all online services would increase in Europe and quality of experience would degrade as routing would be affected.
- a slow-down of innovation as the cost for innovative businesses to serve clients would increase. Adoption of non-European innovation would be hampered by the cost of compliance.

None of these impacts are in line with the goals of the DNA, and they actually go against the EU renewed goals of competitiveness and innovation. The DNA seems at odds with itself, as if higher usage of data by end users and businesses was inherently bad while simultaneously encouraging the deployment of higher capacity networks…

---

[1] European Commission: Legislative proposal for a Digital Networks Act (2026)

[2] IP interconnection refers to the arrangements through which different networks exchange internet traffic with each other. Every time a user accesses a website, sends an email, or streams a video, data travels across multiple independently operated networks. IP interconnection is the set of commercial and technical agreements that allow these networks to hand traffic to one another, ensuring that content reaches its destination regardless of which network the sender or receiver is connected to. These arrangements have historically developed through voluntary commercial negotiation rather than regulatory intervention.

[3] The DNA uses the term providers of "public electronic communications networks" which includes but is not limited to telecom operators.

[4] The DNA includes CAPs in the generic term "other undertakings".

1 Introduction

The European Commission published a legislative proposal for a *Digital Networks Act* (DNA) on 21 January 2026[5]. This text is currently subject to the ongoing co-legislative procedure, involving both the European Parliament and the European Council (Member States).

The DNA proposal follows a period of several years of discussion on the telecoms and connectivity ecosystem, during which the European Commission (also referred to as "Commission") placed focus on, inter alia, what it suggests are issues around IP Interconnection:

- Back in 2023[6] the European Commission referred to a "fair contribution by all digital players", de-facto embracing the inaccurately named "fair share" debate, really a suggestion of imposing payments to major telecommunications operators (at least by improperly-called "large traffic generators".) Feedback from large portions of the communications industry, business and consumers was overwhelmingly negative.[7]

- Then in its 2024 White Paper *How to master Europe's digital infrastructure needs?*[8] – in the name of a perceived convergence between telecom and cloud – the Commission suggested expanding the scope of telecom regulation, potentially subjecting private networks and Content Delivery Networks (CDNs) to the regulatory obligations designed to ensure fair participation in the voice and broadband access markets. This idea was rejected by the large majority of stakeholders participating in the associated public consultation[9].

- In its 2025 *Call for Evidence*[10], the Commission envisaged introducing a mandatory arbitration mechanism to address IP Interconnection disputes, despite recognising that there are very few[11]. A large number of organisations, once again, responded to the call for evidence, maintaining that the IP interconnection market needed no regulatory intervention. 84 organisations and civil society groups – including consumer associations – wrote[12] to the Commission explaining how regulation of IP interconnection would harm "European consumers, businesses, digital rights and the sustainability of the creative and cultural sectors" and calling "on EU policy makers to reject such a regulatory intervention that could introduce direct or indirect payment obligations on Content and Application Providers (CAPs), whether through a mandatory dispute resolution mechanism, mandated negotiations or any other mechanism effectively introducing network usage fees".

The paradox of these envisaged measures is that the European Commission has not demonstrated problems with the way the IP Interconnection market works. In its landmark *Report on the IP interconnection ecosystem*[13] (2024), the Body of European Regulators for Electronic Communications (BEREC) shows that the market is highly competitive, and that issues, when they exist, involve vertically integrated telecom operators present on both the retail Internet access markets (fixed and mobile) and IP Transit markets. As pointed out by the European Parliamentary Research Service (EPRS), "whereas the impact assessment [of the

[5] European Commission: Legislative proposal for a Digital Networks Act (2026)

[6] European Commission: Consultation on The future of the electronic communications sector and its infrastructure (2023)

[7] Responses to the exploratory consultation can be found here: https://digital-strategy.ec.europa.eu/en/library/results-exploratory-consultation-future-electronic-communications-sector-and-its-infrastructure

[8] European Commission White Paper: How to master Europe's digital infrastructure needs (2024)

[9] Unlocking the Future of Connectivity: An In-Depth Analysis of the Public Consultation on the White Paper (Political Intelligence, 2024)

[10] European Commission Call for Evidence, June 2025

[11] Plum Consulting: Exploring the negative impacts of legally mandated dispute resolution in IP Interconnection (2025)

[12] Net Neutrality in the upcoming Digital Networks Act (BEUC, 2025)

[13] BEREC Report on IP Interconnection Ecosystem (2024)

DNA] mentions briefly the lack of cooperation between actors in the connectivity ecosystems, it neither addresses the issue properly nor discusses policy options."[14]

Since 2023, the Commission appears to have placed particular emphasis on addressing concerns around IP Interconnection, despite lack of evidence of a systemic issue in this area. Now that the DNA legislative proposal is published, how does it align with these repeated attempts at regulating IP Interconnection? The purpose of this short report is to analyse the actual text of the DNA legislative proposal in light of previously identified risks in regulating IP Interconnection (section 2.) Then we will summarise these risks as highlighted by previously published studies (section 3.) Finally, we will look at how the DNA might be altered, for better or worse, during the legislative process (section 4.)

2 What the DNA legislative proposal says

The DNA is a very comprehensive and wide-ranging piece of legislation. Two sections in particular explicitly relate to the IP interconnection issues discussed above, and impact the relationships between telecom operators and other undertakings, ie. businesses of all sizes that rely on telecom networks to satisfy their customers' demands.

- Article 9 and related articles on the general authorisation, which define the types of businesses subject to this regime and the related obligations;
- The second is Articles 191-193, which establish a conciliation mechanism to make relationships between providers of electronic communication services and/or other undertakings more efficient.

Internet traffic delivery

There are three primary ways in which traffic can be delivered over the internet.

Transit is a paid service providing a network with connectivity to the whole of the Internet;

Peering is a transactional interconnection between two networks whose owners decide it's in their mutual interest [(a)] to exchange traffic directly. Peering, in 99% of cases is not a paid transaction since it's mutually beneficial;

Content Delivery Networks [(b)] (CDNs) are distributed sets of servers that cache content likely to be most wanted by end-users as close to said users as possible to minimise traffic flows. Content and Application Providers pay for CDN services, but in some instances private CDNs can be deployed as a direct transaction between content providers and ISPs, the specifics of which are protected by contractual confidentiality.

See Annex 1 for more details

(a) The mutual benefit is derived from neither party having to pay transit for traffic and by a significant increase in the quality of traffic routing between these two networks.

(b) NIS2 legislation defines CDNs as "content delivery network" means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers."

2.1 The proposed expansion of the general authorisation regime

The general authorisation regime consists of a series of specific obligations, listed in Article 9 of the DNA. They include:

- compliance with resilience, critical communications, standards and specifications and cybersecurity rules (Article 9.4 a. to d.),
- access to data for lawful interception as in Article 9.4 e.,
- compliance with interconnection requirements outlined in Article 66 (Article 9.4 g.),
- interoperability of services as in Article 9.4 i,
- administrative charges in accordance with Article 12 (as in Article 9.4 j.)

This same Article establishes the type of providers subject to the general authorisation. In particular, Article 9.2 states the following:

> *The general authorisation regime shall apply to providers of public electronic communications services and providers of electronic communications networks used,*

[14] European Parliamentary Research Service Initial Appraisal of a European Commission Impact Assessment (2026)

wholly or mainly, for the purpose of providing electronic communications services or information society services available to the public.

The inclusion of "*providers of electronic communications networks used [..] for the purpose of providing [..] information society services available to the public"* is a fundamental change from the scope of the European Electronic Communications Code (EECC), and it has potentially wide-ranging consequences. In essence, this article:

- extends the scope of the general authorisation in such a manner that the DNA covers a massive range of service providers that rely on private networks to deliver electronic communications services to third parties or private networks that carry information society services. This could include a wide range of B2B and B2C services such as websites, online newspapers (and apps), banking apps, Virtual Private Network services, e-commerce stores, email services, online storage services, etc.
- defines the undertakings that would be included in the scope in an extremely vague manner that would give both the European Commission and national regulators huge latitude to include virtually any provider or carrier of electronic communication services in its scope, from day one or later down the line. Notably, the DNA does not define what information society services are[15].

This legal uncertainty is compounded by an internal contradiction within the DNA itself. Recital 43 explicitly excludes "networks mainly used for private, internal or closed, predetermined user group communications" and "internal links between communications infrastructure facilities not mainly intended for publicly available digital services." Yet the disconnect between the recitals and the binding articles creates significant legal uncertainty: while the recitals suggest a narrow intent, the operative text enables a far broader interpretation.

In particular, when it comes to the different architectural components of the internet, many of its building blocks – built as or relying on private networks – could fall in scope of the general authorisation, including but not limited to:

- Internet Exchange Points that are not networks per se, but carry traffic that provides electronic communications services or information society services available to the public;
- Transit providers, private networks designed to carry traffic to the entirety of the internet, which obviously includes all manners of electronic communications services or information society services available to the public;
- Content Delivery Networks, that are not networks per se, but rather a distributed set of servers which cache content (i.e. information society services) close to end users.
- Private Networks, operated by all types of multi-site companies for their own internal operations, but also used in the process of delivering information society services (e.g. e-commerce, banking services, travel booking services, etc.) to the public.

Furthermore, the current wording of Article 9.2 is so vague that it could also include many businesses that are unrelated to electronic communications, such as B2B IT service providers, data centre operators, cloud providers, broadcasters, content providers, banks, fintech firms, transport operators, and utilities (all subject to their own legal regime in the EU, most of which already harmonised).

As it stands, the broad and unspecified definition gives NRAs and the European Commission excessive latitude to include more or less any participant in the ecosystem in the scope of general authorisation, with, furthermore, a very real risk of fragmentation as different NRAs decide to bring in scope different market participants.

[15] However, directive (EU) 2015/1535 does define "information society services" as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*"

The consequences of an inclusion in the general authorisation regime are many; the most significant ones are the following:

- Added regulatory burden: An added regulatory burden, in particular when it comes to notification, reporting and compliance obligations (not to mention corresponding fees for notified entities). This extension also risks regulatory overlap by duplicating existing, tailored frameworks such as NIS2 or DORA. These overlapping burdens would weigh disproportionately on smaller players who have less resources to handle such an administrative load;

- Interconnection obligations: Actors falling in scope and classified as public electronic communications networks (ECNs) would in addition be subject to interconnection and access obligations as detailed in Articles 66-69. These articles are clearly designed to arbitrate contentious relationships between public electronic communications providers, in particular to help pry open monopolies or dominant position operators which do not exist in the IP Interconnection market. However, crucially, being subject to the general authorisation as public ECNs means that an NRA can force interconnection among players, which in the IP world is absurd since peering is a voluntary, mutually beneficial relationship. Additionally, as different NRAs make different decisions on classifying certain actors as public ECNs, this creates additional fragmentation;

- Furthermore, Article 189 gives the NRA the power of arbitration in such interconnection disputes, which again would mean that network routing could end up being decided by regulators as opposed to common sense and optimal traffic management. It could also be used by public electronic communication networks as a weapon to obtain payment from peering, going against the historical norm in the market.

If we focus for example on the case of Content Delivery Networks (CDN) and how they could be impacted by the general authorisation regime, we find two troubling consequences:

1. The regulatory burden for CDNs would increase.
2. If classified as public networks, CDNs would be subject to peering obligations (Article 66) and mandatory dispute-resolution (Article 189). A dispute resolution mechanism could easily be gamed by large telecom operators who would argue that CDNs represent a large part of the traffic coming on to their networks (despite the associated cost being minuscule or non-existent[16]), and therefore issue systematic arbitration requests against CDNs. Once large telecom operators get at least one ruling in their favour (probably in countries where government and regulator are amenable to the telco's arguments in the network fees debate), they would play on the precedent setting nature of arbitration to argue that all IP Interconnection negotiations with CDNs everywhere should earn them revenue. Note that the wording of Article 189 is ambiguous and could fold into scope even networks not considered public: the general authorisation in Article 9.4g establishes interconnection obligations, which could be considered sufficient requirement to establish that "other undertakings benefit from obligations of access or interconnection" as per Article 189.

The application of this strategy would lead to cost increases for CDN providers, and cascading price increases for all of their clients, including tens of thousands of European online businesses, applications, newspapers, gaming providers, video-streamers, etc. Simultaneously, quality of experience and latency would be degraded due to arbitration between efficient but expensive routes and less efficient but cheaper ones.

The impact of a similar strategy on transit would obviously be very significant as well, especially since an increase in transit costs – due to imposed network fees through dispute

[16] From Felten, Kenny and Webb's 2025 study *European telecom operators are well placed to meet future investment requirements in digital infrastructure*: "The costs of meeting the residual growth in traffic are found to be typically less than 1% of annual network capital expenditure."

resolution – would not only impact the whole internet ecosystem, but also many smaller Internet Service Providers who rely disproportionately on transit to route their customers' traffic.

2.2 The proposed Conciliation Mechanism

Articles 191-193 of the DNA detail a conciliation mechanism between providers of electronic communications networks and unspecified "other undertakings". This is done in the name of "facilitating cooperation on technical and commercial matters", despite BEREC finding no issues with collaboration in the ecosystem, including on issues related to IP interconnection.

Under these new provisions, BEREC would need to issue guidelines on ecosystem cooperation and work with the Office for Digital Networks (ODN, previously BEREC Office) to facilitate ecosystem cooperation.

The mechanism itself relies on the national regulator of the party lodging the request to organise a conciliatory meeting and then report back to BEREC on both the request itself and the proposed conciliatory solution. This assumes that both parties agree to the conciliation, which is not mandatory.

Crucially, the Commission opens up the opportunity to revise the mechanism after 36 months in ways not specified in the DNA. This could include making it mandatory.

While it may seem that the mechanism, in its current non-binding form, is not a threat to the internet ecosystem, it could be gamed even in this current form by large telecom operators wanting to go against the current assessment of BEREC that IP Interconnection is a competitive market that functions in a healthy way. By lodging repeated requests for conciliation, telcos could artificially make it appear as if there are issues *en masse*.

Furthermore, the wording of the conciliation mechanism does not specifically target IP Interconnection, but relates to "technical and commercial arrangements which are subject to the guidelines referred to in Article 191(1)". These guidelines are mentioned in the context of BEREC advising on

> *the application of industry practices and in facilitating cooperation on technical and commercial matters related to the provision of electronic communications services or information society services in an efficient, economically sustainable and reliable way, as well as related to the provision of innovative products and services, to the benefit of end-users.*

This is an extremely broad scope that covers not only IP Interconnection but all matters of contractual and non-contractual relationships between providers of electronic communications networks and virtually any other party in the digital ecosystem. It's not difficult to anticipate the ways in which such a broad definition could be creatively gamed by parties on either side to give the illusion that current relationships have "issues" irrespective of any market reality.

We have highlighted the risks of mandatory arbitration in IP Interconnection above, and this would be a different (and additional) way in which such arbitration could be implemented.

3 Risks associated with the DNA proposals

This section examines how previous research already pointed out the risks associated with DNA proposals leading to mandated arbitration.

The risks identified in Section 2 – scope expansion through Article 9.2 and the conciliation mechanism in Articles 191-193 – did not come from nowhere. Prior to the DNA's publication, at least two independent studies had already analysed the policy directions signalled in the Commission's 2024 White Paper and the 2025 DNA Call for Evidence, and reached conclusions that closely mirror the risks now materialised in the DNA's legislative text:

- the 2024 Plum Consulting report "Consequences of EC proposals to extend regulatory scope to the entire digital economy" (Felten, Schoentgen) – which analysed the risks of scope expansion;

- the 2025 Plum Consulting report "Exploring the negative impacts of legally mandated dispute resolution in IP interconnection" (Blanche, Felten, Miller, Alexiadis) – which analysed the risks of mandatory arbitration.

The purpose of this section is to demonstrate that the consequences of the DNA's approach were foreseen, that its risks were identified by independent research before the proposal was published, and that the evidence base consistently points to the same negative outcomes. The risks identified in Section 2 are not speculative – they are well-documented and empirically grounded.

3.1 Expansion of the scope of telecom regulation to other market participants

The 2024 European Commission White Paper expressly suggested expanding the scope of the European Electronic Communications Code (EECC) to market participants other than operators of electronic communications networks and services in the name of convergence and fairness. It did not demonstrate either convergence or unfairness. This is outlined in Scenario 4 of the White Paper:

> *In order to address the converged electronic communications connectivity and services sector and to ensure that its benefits reach all end-users everywhere, the Commission may consider broadening the scope and objectives of the current regulatory framework to ensure a regulatory level playing field and equivalent rights and obligations for all actors and end-users of digital networks where appropriate to meet the corresponding regulatory objectives...*

The DNA would implement this expansion by folding new actors from the digital ecosystem into the general authorisation regime. As explained in 2.1, this would have more significant impact on actors classified as public networks.

A 2024 Plum Consulting study[17] established the consequences of an expansion of scope:

- A significant increase in the cost of being regulated for the newly targeted entities. This would create inflationary pressure on all of the ecosystem's participants from end-users to enterprises to service providers. These cost increases would reverberate throughout the industry as price increases, slowing down adoption of technology solutions and generally increasing the cost of participation in the digital economy.
- Further Internet fragmentation as the cost of regulatory compliance would increase disproportionately for Europe compared to other geographies.
- Finally, questions about the capacity for National Regulatory Authorities (NRAs) to handle such an expansion of their regulatory activities.

These findings directly corroborate the analysis in Section 2.1: the entities identified by Plum as potentially captured are precisely those now at risk under Article 9.2's vague definition. The fact that the DNA's Article 9.2 implements the White Paper's Scenario 4 almost verbatim confirms that the risks identified by Plum were not hypothetical – they are now embedded in proposed legislation.

3.2 Mandated dispute resolution mechanism on IP Interconnection

Prior analysis of the consequences of mandated dispute resolution also exist, in particular in the 2025 Plum Consulting report Exploring the negative impacts of legally mandated dispute resolution in IP interconnection (Blanche, Felten, Miller, Alexiadis.)

The basis for their analysis of a mandated arbitration mechanism in IP Interconnection is the following:

[17] Consequences of EC proposals to extend regulatory scope to the entire digital economy (2024, Felten, Schoentgen)

- the European Commission's White Paper "How to master Europe's digital infrastructure needs?" [18] referring to the potential introduction of a dispute resolution mechanism;
- the European Commission's Call for Evidence[19] indicating the possibility of "empowerment of NRAs/BEREC in creating effective cooperation/a level playing field [in IP interconnection]", and
- specific stakeholders (primarily large ISPs) calling for a Final Offer Arbitration system to be introduced in IP interconnection[20].

The introduction of mandated dispute resolution in the IP interconnection market – as suggested by the above policy analyses – could easily turn into the introduction of network fees. Indeed, as the 2025 Plum analysis[21] details, the mandated nature of the dispute resolution would limit or entirely eliminate the freedom of participants to the IP Interconnection relationship to design their routing, and virtually put an end to free peering as the default win-win IP Interconnection relationship it is today.

Said dispute resolution would potentially affect all providers of content and applications either directly – to force payment for peering – or indirectly, since all traffic delivery services (transit, IXPs, Content Delivery Networks) would likely be targeted as well. Indeed, since CDN content is aggregated from thousands of client companies, any mandated fee to a CDN peering with a telecom operator would have to be borne by the clients of said CDN, hence increasing cost of traffic delivery not only for a few large CAPs but for the entire Internet ecosystem. Similar targeting of transit providers would result in increased transit costs, and subsequently price inflation. Smaller companies would be disproportionately impacted, as would smaller telecom operators, who rely more than larger ones on transit.

The risk of introducing mandatory arbitration in IP Interconnection would be as follows:

- The entire digital ecosystem would be impacted by these levies on traffic. For example, European websites, apps, cloud services, and broadcasters would either pay higher prices for their Internet connectivity, or experience degraded service quality, likely both.
- The price of online services would increase across the entire value chain, leading to slower adoption of innovative services, particularly in the B2B space where cloud and other productivity services would cost more for a potentially lower quality. European SMEs in sectors such as manufacturing, healthcare or finance would all face higher costs to use cloud services: for example, hospitals relying on cloud-based telemedicine and health records would face higher costs and possibly degraded service due to traffic levies, resulting in lagging video consultations and slower data access, ultimately affecting patient care. Considering digitisation of businesses in Europe is lagging already[22], this would be a step in the wrong direction. Furthermore, adoption of innovative technologies such as AI would be slowed down significantly.
- Internet traffic efficiency and resilience would be harmed: where interconnection decisions now are made on the basis of technical quality, reliability, resilience and minimising cost, the burden of regulated dispute resolution would lead to slow, high-friction negotiations, increased costs, and encourage sub-optimal network architectures, designed to avoid or mitigate regulated network fees.

Again, we find that the European Commission was forewarned of the consequences of this policy change, but has nevertheless pushed forward in the DNA.

In summary, the two independent studies reviewed in this section reached conclusions that are now directly confirmed by the DNA's legislative text. The 2024 study predicted that scope

[18] European Commission White Paper: How to master Europe's digital infrastructure needs (2024)

[19] European Commission: Call for Evidence, 2025

[20] Strengthening Europe's digital infrastructure to enable our digital future, Telefonica (2023)

[21] Plum Consulting: Exploring the negative impacts of legally mandated dispute resolution in IP Interconnection (2025)

[22] According to the Digital Economy and Society Index, 2024, less than 60% of SMEs (10-249 employees) have at least a basic level of digital intensity

expansion would capture private networks, CDNs, and digital service providers – Article 9.2 does precisely this. The 2025 study predicted that mandatory arbitration would function as a vehicle for network fees – Articles 191-193 create precisely this pathway. The consistency between predictive research and legislative reality strengthens the evidence base for the risks detailed in Section 2 and underscores the urgency of addressing them during the legislative process.

4 How might things evolve during the legislative process?

It is very difficult to anticipate how the legislative process may go, so let us just highlight a few ways in which things could be improved and risks mitigated or averted.

When it comes to the proposed **extension of the general authorisation regime**, the two core issues are the lack of justification for such a widening of the scope of the DNA compared to the EECC, and the extremely vague definition of who, outside of providers of electronic communications networks and services to the public, could also be in-scope.

In absence of a clear justification of the scope extension, this measure looks like a complexification of regulation as opposed to a simplification. Some European Commission representatives have mentioned in public that these measures are included primarily in order to ensure resilience and reliability across the Internet ecosystem. If that is the case, the measure should be focused on ecosystem participants identified as ***single points of failure*** for services ***vital to the end-users***. This would considerably narrow the definition. The European Commission would also need to demonstrate that other existing pieces of European legislation (like NIS2 or the upcoming Cybersecurity Act) are not better vessels for such measures. In particular, CDNs and private networks can be explicitly excluded from the scope of Article 9.2. to avoid legal interpretation subjecting them to the interconnection obligations of Article 66 and the dispute resolution procedures of Article 189.

When it comes to the proposed **conciliation mechanism**, it's hard to argue for its very existence in absence of widespread disputes. The simplest way to mitigate its risk would be to remove this conciliation mechanism altogether. At the very least, the revision clause should be removed so that there is no risk of this mechanism becoming mandatory.

5 Conclusions

The proposals in the DNA that push for an expansion of scope the scope of general authorisation or directly target the IP Interconnection market are not justified, vaguely defined and their impact has definitely not been correctly assessed. While they may not have been designed to introduce a form of network fees regime, they certainly carry a risk that parties intent on network fees will leverage them to obtain such a regime.

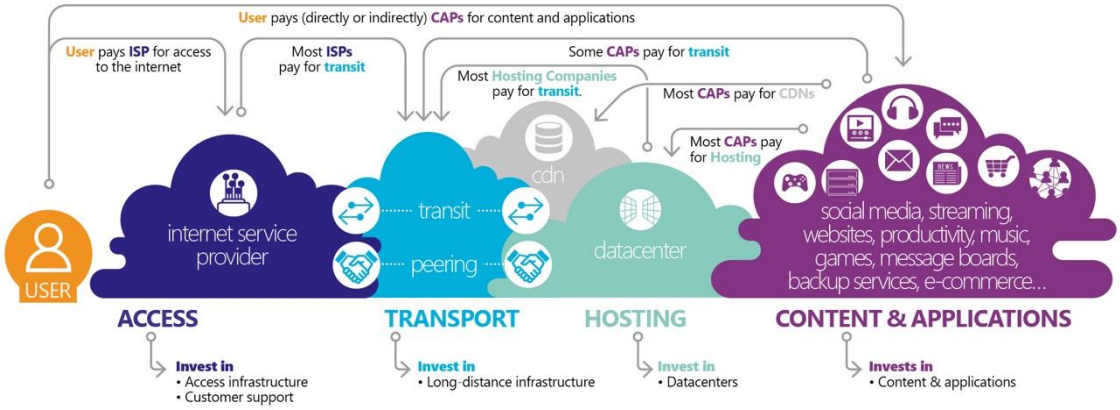
The consequences to the European Internet ecosystem – and the European economy more broadly can be summarised as follows:

- Increased costs for businesses: The cost of doing business online in the EU will increase through the inevitable targeting of Content Delivery Networks and Transit providers, both key components of ensuring low-cost, high-quality flow of Internet traffic. The ripple effect of these cost increases will impact small businesses, innovators and start-ups disproportionately by increasing the cost to reach clients and/or spread the use of their technologies. This runs counter to the EU's stated objectives on competitiveness and digitisation
- Increased costs for consumers: The cost of purchasing online services in the EU will increase as providers pass on their own cost increases to customers and businesses. This will slow down adoption of new services and technologies as well as hamper the adoption of faster broadband solutions since the contents and services they connect with will be less affordable. This will feed inflationary trends.
- Degraded user experience: The quality of experience and resilience on online services will be degraded as decisions that affect traffic routing will no longer be driven by optimal and most resilient options but rather by cost arbitrations and the impositions of mandated dispute resolution or conciliation. This directly contradicts the Commission's stated objectives of strengthening Europe's digital infrastructure.

The DNA has an in-built suspicion that cooperation between public electronic communications network providers and other undertakings is inefficient, and introduces measures to address this unsubstantiated axiom. This creates a strange paradox in which, at the same time the European Commission argues for better, faster and higher capacity networks, it seems to regard additional traffic as unwanted. But traffic is generated by consumers and businesses asking for services enabled by their broadband access products, not parasitic content sneakily entering access networks unwanted. Europe should embrace increased usage of digital innovation and the traffic it represents (which telecom networks are more than capable of handling[23]) rather than put hurdles that can only slow down its own digitisation.

[23] See Three ways the Digital Networks Act would harm the Open Internet, Mike Blanche, 2025

ANNEX 1: Relationships between players in the broader communications ecosystem



- End-users pay Internet Service Providers (ISPs) for access to the internet, and they pay – directly or indirectly – Content and Application Providers (CAPs) for the services they desire.
- ISPs invest in access infrastructure and customer support to deliver access to the internet to end-users.
- The data between networks flows through multiple roots: transit, a paid for service that connects to the entire internet, peering, direct interconnection between two networks, and Content Delivery Networks (CDNs) set-up or paid for by CAPs. The vast majority of participants in the digital economy pay for transit, and transport providers in general invest in long-distance infrastructure.
- The data is primarily hosted in datacenters, paid for by CAPs.
- CDNs offer content distribution across the Internet, paid for by most CAPs.
- CAPs earn money from end-users, pay for content hosting and distribution, and invest in the content and applications they offer.