**REGIONAL ADMINISTRATIVE COURT OF LAZIO**

**ROME**

**SECTION IV – Case No. 13724/2025**

**STATEMENT OF INTERVENTION *IN SUPPORT***

in the interests of the **Internet Society**, with its registered office at 1551 Emancipation Highway, Suite 1506, Fredericksburg, Virginia 22401, United States of America ("**ISOC**" or "**Association**") represented and defended, including with separate powers, by Mariangela Di Giandomenico, Solicitor (Tax Code DGNMNG75H42L103H; PEC mariangeladigiandomenico@ordineavvocatiroma.org) and by Alessandro Amato, Solicitor (Tax Code MTALSN93S23H501J; certified email alessandroamato1@ordineavvocatiroma.org), pursuant to a power of attorney drawn up before a notary on 6 March 2026 and apostilled in Virginia, United States of America (US) on 17 March 2026, (**doc. 1**) with digital domicile at the certified email addresses of the aforementioned counsel.

*– Intervener in support –*

**in civil case no. 13724/2025 brought by:**

**Netflix International B.V.** (registered in the Netherlands, VAT No. NL853746333B01), with its registered office at Karperstraat 8-10, 1075 KZ, Amsterdam, Netherlands ("Netflix"), in the person of its *pro tempore* legal representative Georg Wilfried Nolte, represented and defended by the lawyers Ernesto Apa, Maria Vittoria La Rosa, Elena Mandarà and Micael Montinari;

*– Applicant –*

**Against**

the Communications Regulatory Authority – AGCOM (hereinafter also "AGCOM" or "the Authority"), in the person of *its current* legal representative;

*– Respondent –*

**and against**

**the Italian Internet Providers Association** ("AIIP"), with registered office at Via Caldera 21, 20153 Milan (MI), (VAT No. 07549520968, Tax Code 97166260154), in the person of its *pro tempore* President;

notifying

**the Ministry of Enterprise and Made in Italy** (Tax Code 80230390587), in the person of the *current* Minister, represented and defended by the Attorney General's Office, with its registered office *by operation of law* in Rome, Via dei Portoghesi 12;

and with the intervention of

*as opposing party:*

**Wind Tre S.p.A.**, in the person of its *pro tempore* legal representative, represented and defended by lawyers Sara Fiorucci and Roberto Santi, with digital domicile as per the certified email (PEC) on the Public Registry;

**Italian television networks – R.t.i. S.p.A.** and **Elettronica Industriale S.p.A.**, represented by their respective legal representatives *for the time being*, represented and defended by solicitors Massimiliano Molino, Stefano Previti, Giuseppe Rossi and Vincenzo Colarocco, with a digital address as per the certified email (PEC) on the Public Registry;

**FOR THE ANNULMENT**

- of Resolution No. 207/25/CONS, adopted by AGCOM on 30 July 2025 and published on the Authority's official website on 5 August 2025, entitled "Review of the conditions for the applicability of the general authorisation regime provided for by the Electronic Communications Code to Content Delivery Networks (CDNs)", together with Annex 1 (**"Resolution 207**" – **doc. 2**);
- as well as, to the extent necessary, any other act that is a prerequisite for, connected to or consequential to the contested acts, even if not known, including Resolution No. 55/25/CONS and annexes (**doc. 3**), concerning the launch of the public consultation.

**FACTS**

**1.** By Resolution No. 55/25/CONS (**"Resolution 55**", doc. 3), AGCOM had launched a public consultation *"to assess the conditions for the applicability of the general authorisation regime provided for by the Code to Content Delivery Networks (**CDNs**)*", raising considerable concerns, given that in no Member State of the European Union where Directive (EU) 2018/1972 (European Electronic Communications Code – "**EECC**") – transposed in Italy by Legislative Decree 207/2021, which amended Legislative Decree 259/2003 (Electronic Communications Code – "**Code**") – has the installation and/or use of CDNs ever been deemed subject to the requirement to obtain a general authorisation.

**2.** Despite the various submissions made during the public consultation opposing this regulation, AGCOM adopted Resolution 207 (doc. 2) on 30 July 2025, setting out ***the "Review of the conditions for the applicability of the general authorisation regime provided for in the Electronic Communications Code to Content Delivery Networks (CDNs)***" ("**Resolution 207**"). Resolution 207 confirms what was already anticipated in the public consultation, namely that CDNs, regardless of their configuration or the distribution model chosen, are to be regarded as a public electronic communications network where they are used to provide services accessible to the public. Consequently, Resolution 207 establishes the applicability to CDN *providers* of the general authorisation regime provided for in Article 11 of the Code, which applies to providers of electronic communications networks and services.

**3.** In an appeal filed on 30 October 2025, Netflix challenged Resolution 207, as well as Resolution 55, as a prerequisite act, seeking their annulment.

In particular, Netflix, highlighting its investment in the creation of a private CDN, through a network of servers distributed across the country, to improve the quality of its service for end-users, argued that Resolution 207 was unlawful, on the basis of seven detailed legal grounds.

* * *

ISOC, a non-profit association founded on 11 December 1992 in the United States of America, incorporated by the Articles of Incorporation filed as Filing Number 924447 with the *Department of Consumer and Regulatory Affairs, Government of the District of* Columbia (**doc. 4**),- as represented and defended above, in view of the association's objectives [see *above*], has an indirect and derivative interest in supporting the unlawfulness of Resolution 207 and the grounds for appeal put forward by Netflix and, therefore, intervenes in the present proceedings *in support* of the appeal brought by Netflix itself, which it considers well-founded in fact and in law for the following grounds of

**LAW**

**I. PRELIMINARY. ON THE LEGITIMACY AND INTEREST OF THE INTERVENER**

**1.** ISOC, founded by some of the early pioneers of the Internet, is a charitable, non-profit association whose purpose is to <u>support</u> and <u>promote the development of the Internet globally</u>, fostering coordination and collaboration regarding Internet infrastructure, technologies, standards and applications. ISOC recognizes that the Internet is a global technical infrastructure and constitutes a resource that enriches people's lives and fosters their development in today's society.

To this end, ISOC fosters global coordination and collaboration on issues, *standards* and applications relating to and connected with the Internet. As a global non-governmental organisation, ISOC believes that the Internet should be accessible and available to everyone. ISOC aims for an Internet that is (i) open, (ii) globally connected, (iii) secure and trustworthy. Furthermore, ISOC supports communities that are currently excluded from Internet access, promoting connections, including between these communities via the Internet.

In this context, ISOC promotes the development and use of open infrastructure, technologies and *standards* for the Internet and also supports policies aimed at the protection and development of the Internet, not least because of the countless benefits it brings to society.

Given the purposes for which it was established and in light of the objectives it sets itself, ISOC therefore has a genuine interest in the annulment of the measures imposed on Netflix. As is also demonstrated in the technical document prepared by ISOC and attached hereto (doc. 5), the local presence of CDNs offers measurable benefits that Resolution 207, by reclassifying CDNs as electronic communications networks, inevitably compromises. as the CDNs reduce latency, lower transit costs for Internet Service Providers, increase resilience against outages and attacks, and enabling the delivery of high-performance services like e-government, telemedicine, and distant learning. Should the reclassification discourage the local distribution of CDNs, the benefits above mentioned would diminish, and Italian users would experience a decline in service quality as content distribution would shift to more distant infrastructure.

Indeed, Resolution 207, by  requiring CDN operators to obtain a general authorization in advance inevitably imposes a series of additional obligations which have the effect of discouraging the deployment of servers within the country and increasing reliance on cross-border content distribution. Resolution 207, in fact, insofar as it introduces, as will be seen below, administrative burdens for the use of CDNs, limits the quality of Internet access and use , by raises the costs of the Internet and limits the investments in the sector aimed at promoting the development of content transmitted via the Internet, also undermining the purposes for which ISOC was established limiting the Interne tperformance provided to users and the investments in the sector aimed at promoting the development of contents delivered via the Internet.

The approach of **Resolution 207** is *unique* at European level and sets a clearly negative precedent for the development of and widespread access to the most advanced content and services transmitted over the Internet, as will be explained in more detail *below*. In effect, this regulation would likely result in a transfer of traffic currently exchanged and *cached* within Italian territory to longer and less reliable international routes, weakening the signal and reducing its strength, with a consequent deterioration in the services that are generally accessed by users.

Furthermore, the clear diversion of traffic away from national interconnection points leads to an inevitable reduction in investment in local infrastructure, limiting in the long term the availability, access, services and quality offered to users. The architecture resulting from this arrangement would therefore be characterised by reduced optimisation and greater dependence on international transit capacity due to the lack of local *caching* infrastructure. This is likely to result in a reduction in the network's capacity to manage traffic efficiently, especially during periods of high demand or in the event of outages caused by technical problems or malicious attacks, , reducing performance for users.

The ultimate consequence of these changes would therefore be a deterioration in the quality and, consequently, the usability of the services delivered via the Internet to users. In essence, all services (including Internet services used by public entities or *streaming* services) would experience slower loading times, poorer *streaming* quality during peak periods, and greater susceptibility to interruptions in international connectivity.

The administrative burden imposed creates a regime of unequal treatment even in relation to users in other Member States of the European Union, where the rule imposed by the Authority has not been adopted, as it is contrary to the rules and principles at European level.

For this reason too, together with the arguments already put forward regarding ISOC's *mission* and the role it plays, the conditions regarding ISOC's standing and interest in intervening in this case *in support* of the appeal brought by Netflix are fully met, since the provisions contained in Resolution 207 effectively constitute an obstacle to the proper dissemination of content transmitted via the Internet and to the development of the Internet itself in Italy, in accordance with the objectives pursued by ISOC.

Hence the full admissibility of the intervention, given also the connection with the appellant's interest.

As is well known, the conditions for bringing an intervention *in support* – all of which are met in the present case – have been repeatedly recalled in administrative case law (see, *inter alia,* Council of State, Section IV, judgment of 15 July 2021, No. 5339), according to which parties holding subjective positions dependent on that of the applicant or who have an indirect interest in the annulment of the effects produced by the contested act, and therefore those who have an interest dependent on that of the applicant, in so far as it is ancillary to it, are entitled to intervene (Council of State, Section IV, 29 November 2017, judgment No. 5596; Council of State, Section III, judgment of 14 December 2016, No. 5268; Council of State, Section III, judgment of 26 October, No. 4487; Council of State, Plenary Session, judgment of 28 January 2015, No. 1).

Therefore, the fact that the intervener's legal position is strictly dependent on the outcome of the proceedings – that is, the existence of an indirect interest in the final decision, as in the present case – constitutes grounds for justifying the intervener's participation in the proceedings.

## II. ON THE MERITS OF NETFLIX'S APPEAL

### 1. <u>Introduction.</u>

Netflix has challenged Resolution 207, putting forward the following legal grounds:

*I. Lack of jurisdiction on the part of AGCOM. Breach and misapplication of Article 11 of Legislative Decree No 259 of 2003. Breach and misapplication of Articles 5 and 12 of Directive (EU) 2018/1972.*

*II. Breach and misapplication of Article 97 of the Constitution. Breach and misapplication of Article 1 of Law No 241/1990. Breach and misapplication of the principle of loyal cooperation between public administrations. Breach and misapplication of Article 4 of the Treaty on European Union. Infringement and misapplication of Article 3 of Directive (EU) 2018/1972. Abuse of* *power due to failure to conduct a proper investigation, misrepresentation and manifest injustice, misuse of power.*

*III. Absence of the conditions for subjecting CDNs to general authorisation. Breach and misapplication of Articles 2 and 11 of Legislative Decree No 259 of 2003. Breach and non-application of Article 2 of Directive (EU) 2018/1972. Abuse of power due to misrepresentation of the facts, failure to conduct a proper investigation, unreasonableness and manifest injustice.*

*IV. Misuse of powers due to unreasonableness, manifest injustice, and inconsistency. Breach of the principle of freedom of establishment under Article 56 TFEU. Breach of the principle of proportionality and Article 5 TEU.*

*V. Infringement and misapplication of Article 5 of Directive (EU) 2015/1535 and recital 17 of Directive 2010/13/EU. Failure to notify the draft technical regulation.*

*VI. Infringement and misapplication of Articles 2, 3 and 13 of Directive 2010/13/EU, as amended by Directive 2018/1808/EU. Infringement and misapplication of Articles 1 and 3 of Directive 2000/31/EC*".

ISOC considers that Resolution 207 is unlawful and an obstacle to the pursuit of the Association's mission; it therefore supports the grounds of appeal raised by Netflix as they are well-founded and thus worthy of acceptance for the reasons set out by the applicant, as well as for the following considerations which further support those reasons, subject to further submissions and objections during the proceedings.

*

**<u>2. Concerning the absence of the conditions for subjecting the CDN to general authorisation – and the infringement and misapplication of Articles 2 and 11 of the Electronic Communications Code.</u>**

**2.1.** ISOC concurs with Netflix's arguments regarding the nature of CDNs, arguments upon which the third ground of appeal is based.

In particular, the term "*Content Delivery Network*" has been defined by several authoritative standards bodies. The Internet Engineering Task Force ("**IETF**"), the leading standards body for Internet technologies, has described a CDN as a technology that enables *"the caching of content closer to the edge of a network, so that a given* *piece of content can be served from a CDN proxy* [i.e. a server that stores a copy of the content close to the user] *to multiple user agents* [i.e. devices such as browsers or media players] *(and their end users) without passing through the network core multiple times (i.e. from the content origin to the proxy). This contributes to reducing bandwidth costs for the NSP* [network service provider] *and improving the quality of experience for end users*".[1]

CDNs also enable the replication of popular content across many proxies, allowing it to be served simultaneously to a large number of user agents. The Telecommunication Standardization Sector of the International Telecommunication Union (**ITU-T**), a specialized agency of the United Nations, describes CDNs in a similar way in functional terms: "*it is a system of distributed servers that share content (e.g. web pages, files, video and audio) with users based on predefined criteria such as the geographical location of users, the status of the content distribution server and the IP network connection*." The European Telecommunications Standards Institute (**"ETSI"**), on the other hand, has defined CDNs as: "*a collaborative set of components, in which content is replicated across multiple mirror servers to ensure transparent and efficient delivery of content to end-users*". AGCOM itself, moreover, defines a CDN in extremely concise terms as *"networks consisting of a set of geographically distributed servers, designed to speed up and optimise the delivery of content to end* users" (see point 1.1 of Resolution 207).

All these definitions (including that adopted by AGCOM) place the emphasis <u>on the optimisation and distribution of content</u> through the existing network infrastructure. Indeed, all definitions consistently characterise CDNs as sets of servers that use techniques such as *caching* and geographical distribution to <u>optimise content distribution</u>. Given the highly technical nature of the matters, it is deemed useful to provide a brief technical memorandum, drawn up by ISOC, to further support the arguments regarding the functioning of the internet and CDNs (doc. 5).

**2.2**. Following the public consultation, the Authority decided to confirm in Resolution 207 that CDNs would fall *"within the scope of the definition of an electronic communications network referred to in Article 2 of the Electronic Communications* Code", and

[1] Since 1992, the Internet Society has supported the IETF by providing a corporate home for the IETF LLC - the administrative entity of the IETF - and through annual financial contributions.

to therefore consider the general authorisation regime referred to in Article 11 of the Code applicable to them. However, this interpretation is entirely incorrect, since CDNs do not fall, nor can they in any way fall, within the definition of *'electronic communications* network' within the meaning of Article 2 of the Code, as the applicant also contends.

Pursuant to Article 2(vv) of the Code, *'electronic communications network'* means *'transmission systems, whether or not based on a permanent infrastructure or a centralised management capability and, where applicable, switching or routing equipment and other resources, including passive network elements, which enable the transmission of signals by cable, by radio, by optical fibre or by other electromagnetic means, including satellite networks, mobile and fixed networks (circuit-switched and packet-switched, including the internet), systems for the transmission of electricity by cable, insofar as they are used to transmit signals, networks used for radio and television broadcasting, and cable television networks, regardless of the type of information carried*".

A key element in identifying an electronic communications network is therefore a system's ability to transmit signals: <u>signals, not content.</u> Consequently, a CDN <u>cannot be classified as an 'electronic communications </u>network', given that <u>this definition under the Code is based on the concept of signal transmission systems</u>. CDNs, on the other hand, operate essentially via servers for the purpose of storing and routing the content of the content provider, an activity that certainly cannot be considered comparable to that carried out by the transmission systems used by electronic communications providers, which play an active and prominent role in the transmission and routing of data as opposed to content or which, in any case, perform functions falling within the definition set out in the Code.

<u>Hence the error in Resolution 207, which unlawfully equates CDNs with data transmission networks, subjecting them to general authorisation, in breach of the provisions referred to in the heading of the third ground of appeal.</u>

**2.3.** <u>But there is more</u>: as already argued and as also raised by the appellant, in the rejected and implausible scenario where it were to be considered that CDNs constitute electronic communications networks, Resolution 207 is in any case unlawful in so far as it states that CDNs must *be "regarded as a **public** electronic communications **network**"*.

Public electronic communications networks are defined in Article 2 of the Code as networks used *"entirely or predominantly to provide electronic communications services accessible to the public, which support the transfer of information between network termination points*". Consequently, such an equivalence implies that, according to AGCOM, any web server transmitting content accessible to the public should qualify as a public electronic communications network, the operation of which would therefore require a general authorisation. Furthermore, AGCOM consistently confuses "content" with "signals", whereas the former may, in fact, consist of the latter: <u>an electronic communications network transmits signals</u>, whilst <u>a CDN transmits content</u> which, as such, is not subject to the Code's regulations.

In reality, the legislator has a clear understanding of the distinction between signals and content, as is evident from the fact that it uses the term 'content' <u>exclusively to exclude such</u> content <u>from the scope of the Code.</u> Under Article 1.2(a), in fact, *"The [Code] does not apply to provisions concerning […] services that provide content transmitted using electronic communications networks and services or that involve editorial control over such content*". This concept is reiterated in Article 2(fff), which excludes from the definition of electronic communications services those "*services that provide content transmitted using electronic communications networks and services*". It is, however, <u>undisputed</u>, even in the definition of CDN proposed by AGCOM, that <u>CDNs provide content</u>. As is well known, CDN stands for *Content Delivery Network*: therefore, there can be no doubt that CDNs fall outside the scope of the Code's regulations.

On the other hand, an analysis of Resolution 207 reveals a profound regulatory "confusion". Although Resolution 207 concludes in Article 1 that CDNs would fall *"within the scope of the definition of an electronic communications network referred to in Article 2 of the Electronic Communications* Code", nowhere in Resolution 207 does AGCOM elaborate on the possible applicability of Article 2(vv) of the Code, which contains the definition of an electronic communications network. Instead, AGCOM develops its arguments by referring to entirely different concepts: for example, in point 18 of Resolution 207, AGCOM simultaneously argues that a CDN could "*be considered, from the perspective of the Code, as a 'specific type of network' consisting of equipment that enables the transmission of signals via optical fibres",* but also *"a* 'related resource' *to an electronic communications network that supports the provision of services through that network*".

It is abundantly clear that AGCOM is making an erroneous conflation between a network and a related resource: **a system cannot simultaneously be both an electronic communications network and a related resource.** In fact, Article 2(zz) of the Code defines a related resource as those *"related services, physical infrastructure and other resources or elements related to an electronic communications network or an electronic communications service that enable or support the provision of services via that network or service, or are capable of doing so, including buildings or access to buildings, building wiring, antennas, towers and other support structures, conduits, pipes, masts, manholes and distribution cabinets*". These are, precisely, elements related to an electronic communications network and do not in themselves constitute an electronic communications network.

Obviously, the provision of associated facilities (such as ducts or conduits) does not require any general authorisation. In arguing, therefore, that the CDN may be an associated facility (a hypothesis which, in any case, is not considered tenable), **it is AGCOM itself that rules out the possibility that the CDN could constitute an electronic communications network**.

**2.4.** It is also incorrect to argue that the CDN could be a 'specific type of network'. AGCOM, in fact, derives this category from Article 2(l) of the Code, which contains the definition of 'general authorisation', defining it as *'the legal regime which guarantees the rights to provide electronic communications networks or services and establishes specific obligations for the sector applicable to all types or specific types of electronic communications networks and services, in accordance with this decree'*.

Now, it is unclear on what regulatory basis AGCOM considers that the reference to a specific type of network, within a definition dealing with a different subject, could lead to the conclusion that the general authorisation regime is applicable and allow AGCOM to refrain from verifying the precise definition of an electronic communications network set out in Article 2(vv) of the Code. As correctly argued in Netflix's appeal, in fact, the electronic communications network is a categorised and well-defined concept at national and EU level, and the local regulator is absolutely precluded from adopting a broad interpretation that differs from that derived from a reading of the provision. The reference to 'specific types of networks', contained exclusively in Article 2(l) of the Code, is a mere reference intended to clarify the scope of the general authorisation, which recalls its applicability to every type of electronic communications network, obviously as defined in Article 2(vv) of the Code. This is not – to use the effective wording of the Netflix appeal – "*an open-ended provision that could serve as a lever to stretch the definition of an electronic communications network and include infrastructure not covered by the primary legislation*".

AGCOM, as an independent regulatory authority, exceeds its remit and breaches sectoral legislation by adopting an overly broad interpretation of the primary legislation, namely the Code, which is itself a direct transposition of European legislation (resulting from the adoption of the EECC in Italy). On this point, neither AGCOM nor MIMIT, during the Code's period of validity, have ever interpreted CDNs as electronic communications networks. A regulatory intervention which, in 2025, would amend a key definitional framework such as that relating to electronic communications networks, in the absence of any legislative action in this regard, is therefore flawed. Moreover, there is no record of such an interpretation ever having been adopted in any other Member State, further evidence that it goes beyond the text of the Code.

We therefore agree with Netflix's objections raised in the third and fourth ground of appeal, which we request be upheld as well-founded.

**3.** On the fourth ground of appeal we refer to the arguments set forth by Netflix

**P.Q.M.**

We request that this Honourable Regional Administrative Court, having deemed this application to intervene *in support of the main proceedings* admissible, uphold the appeal lodged by Netflix, with all the legal consequences that this entails.

Rome, 16th July 2026

Avv. Mariangela Di Giandomenico Avv. Alessandro Amato

# ANNEX A: A Technical Primer on the Internet and Content Delivery Networks (CDNs)

How the Internet Works ........ 1
CDNs: What they are and how they work ........ 5
Reclassifying CDNs as Public ECNs: Impact on the Internet ........ 9
Summary ........ 10
Bibliography ........ 12

## How the Internet Works

The Internet is commonly referred to as a "network of networks," reflecting its core purpose of enabling communications across different computer networks. While this is an accurate description, it also downplays the Internet's broader significance. In fact, the idea of interconnecting computer networks predates the Internet, but earlier systems were typically closed, limited to specific organizations, or restricted to particular technologies[1]. By contrast, the Internet represents a fundamentally different approach of a distributed and collaborative model based on open standards, which has enabled it to grow to a global scale. From this view, the Internet is not merely a generic data network or a collection of technical protocols. It is a distinct networking model of voluntarily interconnecting diverse and independent networks in a single global communications system[2].

The Internet can be understood as an infrastructure providing a simple function: the ability to send data packets between computers located in different networks operated by different organizations. The connected computers then rely on shared standards to build applications on top of this infrastructure. For example, computers connected to the Internet created the World Wide Web by adopting the Hypertext Transfer Protocol (HTTP), which web browsers and servers use to exchange web pages. This design, in which the network simply delivers packets while the connected computers decide how to use them, explains why the Internet is often described as a general-purpose technology. The same underlying system supports email, the Web, instant messaging, video streaming, online banking, and countless other applications. The

---

[1] Barry M. Leiner et al., *A Brief History of the Internet* (Internet Society, 2009), https://www.internetsociety.org/internet/history-internet/brief-history-internet/.

[2] Internet Society, *The Internet Way of Networking (IWN): Defining the Critical Properties of the Internet* (2019), https://www.internetsociety.org/iwn/.

choice of what to build and how to use connectivity rests with the connected computers, not with the network itself.

The success of this networking model, in terms of its global reach, capacity for innovation, and continuous evolution, lies as much in its governance as in its technology. The Internet is not centrally controlled but operates through the voluntary adoption of open standards developed by multistakeholder processes[3]. Each network retains autonomy while participating in a larger whole, which creates resilience and adaptability.

To understand how this model works in practice, it is useful to outline three important features. First, the voluntary interconnection agreements through which independent networks come together to form the Internet. Second, the layered architecture that organizes the Internet's technical functions and enables different technologies to coexist. And third, the distinct roles played by various actors that make up the Internet ecosystem.

### Voluntary Interconnections

The Internet is built through the voluntary interconnection of more than 80,000 independent networks. Each one of them makes use of widely adopted open standards to set up their connections and produce a shared platform that allows people all over the world to communicate. These voluntary interconnection agreements are underpinned by market-driven incentives and technical efficiency, and are typically in one of two forms[4]:

- **Transit** is an arrangement by which the transit network agrees to provide its customers with connectivity to the rest of the Internet for a fee. Transit providers act as common intermediaries for the thousands of networks on the Internet that would otherwise have to be directly connected with each other. Some transit providers operate international networks with the ability to move data across the globe. This enables the customer purchasing transit to reach many endpoints without having to physically connect to and negotiate agreements with each one.
- **Peering** is an agreement by which two networks agree to a mutual exchange of traffic to and from users on their own networks (but not via their transit links), usually on a

[3] 'Why the Multistakeholder Approach Works', *Internet Society*, 26 April 2016, https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/.
[4] 'Policy Brief: Internet Interconnection', *Internet Society*, 30 October 2015, https://www.internetsociety.org/policybriefs/internetinterconnection/.

"settlement-free"[5] or no-cost basis. Peering arrangements reduce the amount of traffic a network must send through its upstream transit provider, potentially lowering the average cost of traffic delivery. To facilitate peering, many networks choose to build connections to and participate in various local, regional, and global Internet exchange points (IXPs).

For decades, this model has supported growth in connectivity, traffic and user choice. It has been made possible by continued investment in higher-bandwidth infrastructure and the development of new services, such as video streaming, that respond directly to user demand.

### A Layered Architecture

The Internet is commonly described as a layered system in which different technical functions are separated into distinct but interoperable components. While different models exist[6], a common approach is to describe the Internet in terms of four conceptual layers[7]: the link layer, the network layer, the transport layer, and the application layer. Each layer performs a specific role and interacts with the layers above and below it through well-defined interfaces, allowing innovation in one part of the system without requiring changes to the others[8].

The three lower layers (i.e., link, network, and transport) are collectively concerned with the fundamental task of establishing and managing connectivity between devices. They make it possible for data to move from one endpoint to another, reliably and at global scale, without determining what that data means or why it is being sent.

At the bottom sits the link layer, which encompasses the physical infrastructure (e.g., fiber-optic cables, radio links) and the protocols that directly connect devices over a shared medium (e.g., Ethernet, Wi-Fi). This layer moves raw bits between two directly connected endpoints and is indifferent to what those bits represent.

---

[5] "Settlement-free peering" means that neither party pays the other for the exchange of peered traffic between the two networks.

[6] Several models exist for describing the Internet's layered architecture. The most widely referenced alternative is the Open Systems Interconnection (OSI) model, developed by the International Organization for Standardization (ISO), which divides network communication into seven layers. The OSI model was developed as a general reference framework for network communication and predates the widespread adoption of the Internet. The four-layer TCP/IP model used in this brief more directly reflects how the Internet actually operates in practice.

[7] Robert T. Braden, *Requirements for Internet Hosts - Communication Layers*, Request for Comments RFC 1122 (Internet Engineering Task Force, 1989), https://doi.org/10.17487/RFC1122.

[8] Internet Society, *The Internet Way of Networking (IWN): Defining the Critical Properties of the Internet*.

Above this is the network layer, built around the Internet Protocol (IP), which organizes the raw data into packets and assigns them globally meaningful addresses (i.e., IP addresses) so they can be forwarded across multiple interconnected networks. The network layer's purpose is to provide a shared logical layer across otherwise heterogeneous networks (i.e., networks built on different physical infrastructures and link technologies, such as fiber, Wi-Fi, or mobile systems). In doing so, it promotes reachability by resolving the question of how to identify and reach devices across different networks.

The transport layer builds on that reachability to ensure the reliable and ordered delivery of data between specific applications running on different devices. Without it, the network layer would simply deliver packets with no guarantee they arrive complete, in sequence, or at all. Protocols like the Transmission Control Protocol (TCP) structure communication by tracking each packet, confirming its receipt, and requesting retransmission if any are lost, making it possible for devices to exchange data as a coherent, ordered stream rather than a collection of individual packets.

Finally, the application layer is where connectivity is turned into specific services and human-meaningful functions. Protocols such as the Hypertext Transfer Protocol (HTTP) for the Web, Simple Mail Transfer Protocol (SMTP) for email, and many others define how data is structured, what it represents, and what users can do with it. It is at this layer that developers decide what to use the connectivity for, like supporting a website, a video call, a messaging platform, or an application that has not yet been invented.

In this sense, the Internet's layered architecture separates connectivity from purpose. The network establishes the possibility of communication while the application layer determines what form that communication should take.

### The Role of Different Actors

The Internet ecosystem comprises a multitude of distinct types of actors, each playing a different role in enabling connectivity and content delivery. Importantly, these roles can also be mapped onto the different layers of the architecture described above: some actors operate the infrastructure that makes connectivity possible, while others build services and functions on top of it. For the purpose of this brief, we believe it is important to define the following[9]:

- **Internet Service Providers (ISPs):** ISPs operate at the network and link layers. They own or resell the physical and logical infrastructure (cables, radio links, routing equipment)

[9] 'Policy Brief: Internet Interconnection'.

that brings Internet access to end users. ISPs are the primary point of contact between the layered network infrastructure and end users, who both consume and generate Internet traffic.

- **Transit Providers:** A transit provider also operates at the network layer, but at a different scale. These are large network operators that sell Internet connectivity to ISPs and other networks, enabling traffic to traverse their infrastructure to reach the rest of the Internet. Transit providers are essential for global connectivity.
- **Internet Exchange Points (IXPs):** Physical locations at which many different networks meet to peer and exchange traffic over a common switching infrastructure.
- **Content Providers:** Content Providers operate at the application layer. They are the producers and distributors of Internet content, including media companies, web hosting services, social media platforms, software companies, and others. Content providers make use of the connectivity that ISPs, transit providers, and IXPs collectively provide, but their core activity is determining what form that connectivity takes: what content exists, how it is structured, and what users can do with it.
- **Content Delivery Networks (CDNs)**: CDNs also operate at the application layer, but their role is distinct from that of content providers. Rather than producing content, CDNs optimize content distribution on behalf of content providers. They do this by placing servers in many locations around the world (often inside or close to ISP infrastructure) so that content can be served from a point geographically and network-topologically closer to the end user.

Taken together, these actors form an ecosystem that largely mirrors the layered logic of the Internet's architecture. ISPs, transit providers, and IXPs operate at the link, network, and transport layers by building and maintaining the connectivity infrastructure that enables global communication. Content providers and CDNs operate at the application layer, where that connectivity is put to use by determining what content exists and how it is distributed.

## CDNs: What they are and how they work

The term "Content Delivery Network" has been defined by several authoritative standards bodies.

The Internet Engineering Task Force (IETF), the premier standards body for Internet technologies, has described the role of a CDN as[10]:

- "CDNs allow caching of content closer to the edge of a network so that a given item of content can be delivered by a *CDN Surrogate* [i.e., a server that stores a copy of content near the user,] to multiple *User Agents* [i.e., devices such as browsers or media players] (and their End Users) without transiting multiple times through the network core (i.e., from the content origin to the Surrogate). This contributes to bandwidth cost reductions for the *NSP* [network service provider] and to improved quality of experience for the End Users. CDNs also enable replication of popular content across many Surrogates, which enables it to be served to large numbers of User Agents concurrently."

The International Telecommunication Union Telecommunication[11] Standardization Sector (ITU-T) Recommendation Y.2084 similarly describes CDNs in functional terms[12]:

- "A content delivery network (CDN) is a system of distributed servers that deliver content (e.g., web pages, files, videos and audios) to users based on pre-defined criteria such as the geographic locations of users, the status of the content delivery server and the IP network connection."

The European Telecommunications Standards Institute (ETSI) has characterised CDNs as[13]:

- "A Content Delivery Network (CDN) is a collaborative collection of components, where content is replicated over several mirrored servers in order to perform transparent and effective delivery of content to end users."

These definitions share common elements, consistently characterizing CDNs as collections of servers, employing techniques like caching and geographic distribution, to optimize content delivery. Critically, none of these definitions characterizes CDNs as providing network

---

[10] Brad Cain et al., *A Model for Content Internetworking (CDI)*, Request for Comments RFC 3466, Internet Engineering Task Force (IETF), March 2003, 34, https://doi.org/10.17487/RFC3466.

[11] The International Telecommunication Union (ITU) is a specialized agency of the United Nations.

[12] International Telecommunication Union (ITU-T), *Recommendation Y.2084 :Distributed Service Networking Content Distribution Functions*, June 2015, https://www.itu.int/rec/T-REC-Y.2084-201506-I/en.

[13] European Telecommunications Standards Institute (ETS), *ETSI TS 182 019: Content Delivery Network (CDN) Architecture*, 12 September 2011, https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=37766.

connectivity or operating public electronic communication networks. The emphasis is instead on optimization and delivery of content over existing network infrastructure.

### Different types of CDNs and their deployment

CDNs vary significantly in their architecture, business models, and relationships with other network actors:

- **Public CDNs:** These are operated by third-party providers who offer content delivery services to multiple content providers. Examples include well-known global providers such as Akamai, Cloudflare, and Fastly. Content providers contract with these CDNs to improve delivery of their content to end users.
- **Private CDNs:** Large content providers may operate their own CDN infrastructure to serve their own content exclusively. Major streaming services and technology companies, such as Netflix or Meta, often maintain private CDN infrastructure optimised for their specific content types.
- **Hybrid Arrangements:** Some organisations employ a combination of private infrastructure and commercial CDN services, using different approaches for different types of content or geographic regions. For example, a content provider might keep its video library on its private CDN, while using a third-party CDN to deliver its website pages and promotional graphics.

A critical aspect of CDN operations is that CDNs may or may not have direct relationships with the ISPs that serve end users. For example, a CDN may deploy servers:

- Within an ISP's network (through a commercial arrangement)
- At IXPs (accessible to multiple networks)
- In third-party data centres (connected via transit)
- In entirely different jurisdictions from the end users being served

This flexibility means that a CDN serving users in one country may have no physical presence, no commercial relationship, or not even a direct network connection within that country. The content may be delivered from servers located abroad, traversing multiple networks before reaching the user's ISP.

### The Benefits of CDNs

CDNs provide significant benefits to the Internet ecosystem, end users, and the broader digital economy. Rather than retrieving content from a distant origin server each time a user requests it, CDNs store copies of popular content on servers closer to end users, so that frequently requested material can be delivered quickly and efficiently without re-sending the data over long and expensive links[14]. A closer understanding of these benefits is essential for evaluating the impact of regulatory changes.

**Reduced Latency -** By caching content at servers closer (geographically or topologically) to the end user, CDNs significantly reduce the round-trip time for content delivery. Rather than each request travelling back to the origin server across long, and often costly, transit links, once the content has been cached at the edge server, subsequent users can retrieve it from that cache[15]. This results in faster page load times, more responsive applications, higher-quality video streaming with less buffering, and more stable performance during peak traffic periods. For latency-sensitive applications such as online gaming and real-time communications, where even small delays are immediately perceptible to users, these reductions are particularly critical.

CDNs also enhance overall network efficiency. By caching and distributing content closer to users, they reduce the need for long-haul and cross-border traffic flows and reduce congestion on core links. Traffic that would otherwise traverse multiple networks to reach a distant origin server can instead be served locally, reducing pressure on shared infrastructure. This enables more efficient use of existing capacity without necessarily requiring additional infrastructure investment, benefiting both network operators and end users.

**Enhanced Resilience -** CDNs provide redundancy and traffic distribution, enhancing the resilience of content delivery. Because content is replicated across multiple servers in different locations, the failure of any single server does not prevent access to the content, as traffic is redirected to the next available server. CDNs also help defend against malicious denial-of-service attacks by intercepting and dispersing harmful traffic volumes before they reach the origin server. More broadly, this distributed architecture also allows CDNs to absorb legitimate traffic surges, such as those caused by major live events, without degradation in service.[16]

**Reduced Costs -** CDNs reduce costs for multiple parties in the Internet ecosystem. For content providers, CDNs reduce bandwidth costs associated with serving content directly from the origin server. For ISPs, transit costs fall when CDN servers are deployed within or near their

---

[14] Dennis Weller and Bill Woodcock, 'Internet Traffic Exchange: Market Developments and Policy Challenges', *OECD Digital Economy Papers* 2013 (January 2013), https://doi.org/10.1787/5k918gpt130q-en.
[15] 'Analysing Global CDN Performance', RIPE Labs, 8 August 2019, https://labs.ripe.net/author/emirb/analysing-global-cdn-performance/.
[16] David Belson, 'Holding Steady: How CDNs, IXPs, and Network Providers Help Keep Us Online', *Internet Society*, 13 July 2020, https://www.internetsociety.org/blog/2020/07/holding-steady-how-cdns-ixps-and-network-providers-help-keep-us-online/.

networks, keeping traffic local and avoiding the need to route it across costly long-haul links. More broadly, by serving content close to the user, rather than repeatedly transmitting the same data across long-haul networks, CDNs improve the overall cost-efficiency of content delivery for the ecosystem as a whole.[17]

Local deployment of CDN infrastructure can also support domestic infrastructure development by placing edge servers at IXPs and other local facilities. This strengthens domestic interconnection ecosystems and reduces dependence on foreign backbone capacity, while keeping a greater share of traffic within local networks.[18]

**Improved User Experience -** The cumulative effect of reduced latency, enhanced resilience, reduced costs, and more efficient delivery is a substantially improved user experience. Users benefit from faster access to content and more responsive applications. Studies consistently show that user engagement and satisfaction are strongly correlated with content delivery performance[19].

Furthermore, CDNs support a wide range of performance-sensitive services such as cloud applications, e-government platforms, telemedicine, distance education, and real-time collaboration tools, all of which depend on low latency and reliable delivery. Without the distributed infrastructure that CDNs offer, many of these services would be slower, less reliable, or difficult to deliver at scale, particularly to users in regions further from content origin servers. In this sense, CDN infrastructure is not merely a performance enhancement but an enabling condition for a broad class of modern digital services and future innovations.

## Reclassifying CDNs as Public ECNs: Impact on the Internet

Reclassifying CDNs as public electronic communication networks (ECNs) would have significant negative consequences for Internet performance and investment within Italy. If regulatory obligations designed for access networks were extended to CDNs, providers may reduce or relocate infrastructure to other jurisdictions.

**Disincentivize Server Deployment -** A decline in local deployment would increase reliance on cross-border content delivery. Traffic that is currently exchanged and cached within Italy would instead traverse longer international routes, increase latency, and reduce routing efficiency. This

---

[17] Weller and Woodcock, 'Internet Traffic Exchange'.

[18] Jahangir Hossain, 'Lessons from 100+ IXes', Tech Matters, *APNIC Blog*, 17 May 2016, https://blog.apnic.net/2016/05/17/lessons-100-ixes/.

[19] *Milliseconds Make Millions* (Deloitte Ireland, 2020), https://www.deloitte.com/ie/en/services/consulting/research/milliseconds-make-millions.html.

would shift traffic away from domestic interconnection points and weaken incentives for local peering and infrastructure investment.

**Inefficient Traffic Flows and Reduced Resiliency -** The resulting architecture would be less locally optimized and more dependent on international transit capacity. During periods of high demand, or due to outages or attacks, the lack of nearby caching infrastructure would reduce the network's ability to manage traffic efficiently, affecting end-user performance.

**Lower Quality of Service for Users -** The ultimate consequence of these changes would be a degradation in the quality of Internet services experienced by Italian users. Users would face slower load times, lower streaming quality during peak periods, and greater sensitivity to disruptions in international connectivity. These effects would be most pronounced for latency-sensitive and bandwidth-intensive applications, which represent an increasing proportion of Internet traffic.

## Summary

The preceding sections have described how the Internet functions, how its architecture is organized, the roles different actors play within its ecosystem, how CDNs operate, the benefits they provide, and the consequences that reclassification could have for Internet performance, investment, and the broader policy landscape. The following observations summarize the key considerations emerging from that analysis.

First, CDNs operate at the application layer and are functionally distinct from network operators. The Internet's layered architecture separates the functions responsible for transmitting data between endpoints from those that make use of that transmission capability. CDNs perform their core functions, of caching content and distributing traffic, at the application layer. They do not establish connectivity between end users and content but instead optimize the distribution of content across infrastructure provided by ISPs and transit providers. These are distinct functions, achieved by different technical means and governed by different commercial relationships. CDNs obtain connectivity by purchasing transit, peering at IXPs, or deploying servers within ISP infrastructure, and where some CDN operators use private backbone networks to move content between their own servers, these do not provide connectivity services to third parties.

Second, CDN infrastructure has no fixed geographic or network relationship with end users. CDN servers may be located in different jurisdictions from the users they serve. A CDN may have no physical infrastructure, direct network connection, or commercial presence in the country where an end user is located. The path between a CDN server and an end user may traverse multiple independent networks operated by third parties. This flexibility is central to how CDNs function and to the benefits they deliver, but it also means that regulatory measures in one jurisdiction can simply shift infrastructure and traffic flows elsewhere.

Third, local CDN presence delivers measurable benefits that a reclassification would put at risk. CDNs reduce latency, lower transit costs for ISPs, enhance resilience against outages and attacks, and enable the delivery of performance-sensitive services such as e-government, telemedicine, and distance education. If reclassification were to discourage local CDN deployment, these benefits would diminish, and Italian users would experience degraded service quality as content delivery shifts to more distant infrastructure.

Finally, a reclassification would bring CDNs within the scope of interconnection dispute resolution, aligning with demands that have been repeatedly rejected in European policy debates. These demands have been consistently opposed by BEREC and a broad coalition of stakeholders. Whether such dispute resolution could in practice be used to this end under existing law is likely to remain an open question. Nonetheless, the reclassification aligns with these ambitions and risks enabling operators to leverage their termination monopoly to extract payments, with costs ultimately borne by content providers and end users.

## Bibliography


Belson, David. 'Holding Steady: How CDNs, IXPs, and Network Providers Help Keep Us Online'. *Internet Society*, 13 July 2020. https://www.internetsociety.org/blog/2020/07/holding-steady-how-cdns-ixps-and-network-providers-help-keep-us-online/.

Braden, Robert T. *Requirements for Internet Hosts - Communication Layers*. Request for Comments RFC 1122. Internet Engineering Task Force, 1989. https://doi.org/10.17487/RFC1122.

Cain, Brad, Mark Day, Gary Tomlinson, and Phillip Rzewski. *A Model for Content Internetworking (CDI)*. Request for Comments RFC 3466. Internet Engineering Task Force (IETF), March 2003. https://doi.org/10.17487/RFC3466.

CircleID Reporter. 'EU Internet Advocates Push Back Against Telecom "Fair-Share" Fees'. CircleID, 29 October 2024. https://circleid.com/ posts/eu-internet-advocates-push-back-against-telecom-fair-share-fees.

European Telecommunications Standards Institute (ETS). *ETSI TS 182 019: Content Delivery Network (CDN) Architecture*. 12 September 2011. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=37766.

Hossain, Jahangir. 'Lessons from 100+ IXes'. Tech Matters. *APNIC Blog*, 17 May 2016. https://blog.apnic.net/2016/05/17/lessons-100-ixes/.

International Telecommunication Union (ITU-T). *Recommendation Y.2084 :Distributed Service Networking Content Distribution Functions*. June 2015. https://www.itu.int/rec/T-REC-Y.2084-201506-I/en.

Internet Society. *The Internet Way of Networking (IWN): Defining the Critical Properties of the Internet*. 2019. https://www.internetsociety.org/iwn/.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, et al. *A Brief History of the Internet*. Internet Society, 2009. https://www.internetsociety.org/internet/history-internet/brief-history-internet/.

*Milliseconds Make Millions*. Deloitte Ireland, 2020. https://www.deloitte.com/ie/en/services/consulting/research/milliseconds-make-millions.html.

'Policy Brief: Internet Interconnection'. *Internet Society*, 30 October 2015. https://www.internetsociety.org/policybriefs/internetinterconnection/.

RIPE Labs. 'Analysing Global CDN Performance'. 8 August 2019. https://labs.ripe.net/author/emirb/analysing-global-cdn-performance/.

Weller, Dennis, and Bill Woodcock. 'Internet Traffic Exchange: Market Developments and Policy Challenges'. *OECD Digital Economy Papers* 2013 (January 2013). https://doi.org/10.1787/5k918gpt130q-en.

'Why the Multistakeholder Approach Works'. *Internet Society*, 26 April 2016. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/.