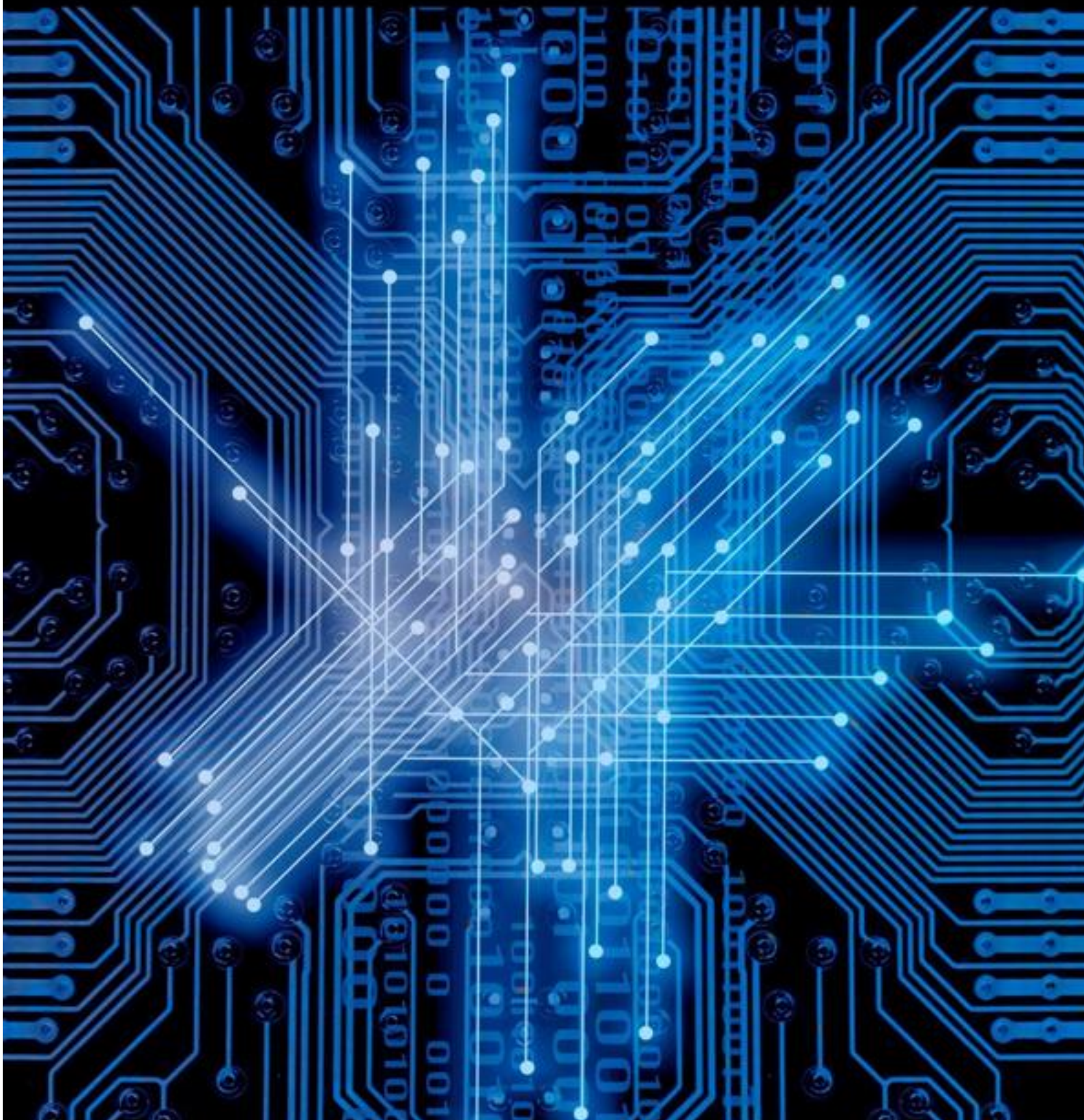
2025

Report on Spain's Supervision of European Regulations on Open Internet Access (Internet Neutrality)



MINISTERIO
PARA LA TRANSFORMACION DIGITAL
Y DE LA FUNCION PUBLICA

SECRETARIA DE ESTADO DE TELECOMUNICACIONES
E INFRAESTRUCTURAS DIGITALES

Report on the monitoring of the implementation in Spain of EU legislation on open internet access (net neutrality)

2025

© Ministerio para la Transformación Digital y de la Función Pública
Calle del Mármol 2 – Parque empresarial Río 55
28005 Madrid

Report by:
The State Secretariat for Telecommunications and Digital Infrastructure
The General Secretariat for Telecommunications and Regulation of Audio-visual Communication Services
https://avancedigital.mineco.gob.es/es-es/Paginas/neutrality-Red.aspx

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

Official Publication ID Number (NIPO): 230260021

Catalogue of General State Administration Publications
https://cpage.mpr.gob.es

CONTENTS

1. EXECUTIVE SUMMARY 1

2. SAFEGUARDING OF OPEN INTERNET ACCESS 5

2.1 THE NET NEUTRALITY PRINCIPLE 6

2.2 ZERO RATING OFFERS 9

2.3 RESTRICTIONS ON THE USE OF EQUIPMENT 10

2.3.1 MODEM / ROUTER PROVIDED BY THE OPERATOR 10

2.3.2 RESTRICTIONS ON THE USE OF CONNECTED EQUIPMENT: TETHERING 15

2.3.3 RESTRICTIONS ON THE USE OF MULTI-SIM CARDS 18

2.3.4 RESTRICTIONS ON THE USE OF SIM CARDS 19

2.4 TRAFFIC MANAGEMENT MEASURES 20

2.4.1 TRAFFIC MANAGEMENT MEASURES EXECUTING COURT RULINGS 22

2.4.2 TRAFFIC MANAGEMENT MEASURES AND 5G TECHNOLOGY 23

2.4.3 REASONABLE TRAFFIC MANAGEMENT MEASURES 25

2.4.4 TRAFFIC MANAGEMENT MEASURES FOR NETWORK INTEGRITY AND SECURITY 35

2.4.5 TRAFFIC MANAGEMENT MEASURES FOR NETWORK CONGESTION 40

2.5 SPECIALIZED SERVICES 43

3. TRANSPARENCY MEASURES TO GUARANTEE OPEN INTERNET ACCESS 49

3.1 CURRENT LEGISLATION 50

3.2 TRAFFIC MANAGEMENT MEASURES IN CONTRACTS 50

3.3 LIMITS ON DATA VOLUMES 52

3.4 INTERNET ACCESS SPEEDS IN CONTRACTS 53

3.5 DISPUTES REGARDING INTERNET ACCESS SPEEDS 56

3.6 COMPLAINTS REGARDING INTERNET ACCESS SPEEDS 62

4. SUPERVISION AND ENFORCEMENT 64

4.1 SYSTEM DESIGNED 65

4.2 RESULTS OBTAINED 67

4.3 INFORMATION PROVIDED BY OPERATORS.....70

5.0 PENALTIES.....71

5.1 SANCTIONING POWER.....72

5.2 POWERS OF INSPECTION AND SUPERVISION.....73

APPENDIX I GLOSSARY OF TERMS.....75

APPENDIX II SUMMARY OF SETELECO CRITERIA ON PRACTICES CONCERNING NET NEUTRALITY.....76

APPENDIX III REFERENCE DOCUMENTS.....79

1. EXECUTIVE SUMMARY

Purpose of the report

The purpose of this report is to describe the monitoring carried out in 2025 by the State Secretariat for Telecommunications and Digital Infrastructure of the Ministry of Digital Transformation and the Civil Service, as well as the main conclusions resulting therefrom.

Specifically, it refers to the provisions of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, known both as the Telecommunications Single Market Regulation (TSM Regulation) and as the Open Internet Regulation (OIR).

Article 5.1 of the TSM Regulation requires National Regulatory Authorities (NRAs) to publish reports on an annual basis regarding their monitoring and findings on compliance with Articles 3 and 4 of the Regulation.

Similarly, Article 76.9 of the General Telecommunications Act (Act 11/2022 of 28 June, hereinafter, the GTA),[1] provides that the Ministry of Economic Affairs and Digital Transformation [whose powers are currently exercised by the Ministry of Digital Transformation and the Civil Service] shall monitor the application of said Article as regards open internet access and shall publish an annual report on this monitoring and the findings thereof and forward it to Spain's National Markets and Competition Commission (CNMC), the European Commission, and the Body of European Regulators for Electronic Communications (BEREC).

Reference documents

Appendix III of this report lists the documents, reports and legislation cited frequently herein.

[1] https://www.boe.es/eli/es/l/2022/06/28/11

Criteria of the State Secretariat for Telecommunications and Digital Infrastructure

Each section of this report details State Secretariat for Telecommunications and Digital Infrastructure (SETELECO) criteria regarding the practices analysed and their compatibility or incompatibility with net neutrality legislation. For greater clarity, a summary of these criteria is provided in Appendix II.

TSM Regulation

The TSM Regulation, which entered into force on 30 April 2016, guarantees end-users a number of rights in relation to internet service providers (hereinafter ISPs or operators). Article 1 thereof asserts that the Regulation "establishes common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights."

The rights recognized in the TSM Regulation are clearly divided into two categories. Those of the first category are intended to guarantee the right to access and distribute information and content, while those of the second are focused on the transparency of these aspects in contracts and the correlative existence of procedures by which to address complaints concerning potential infringements of rights. More specifically, these two categories of rights constitute:

- the rights provided for in Article 3 entitling end-users "to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service."

- The rights regarding transparency set forth in Article 4, which echo those laid down in Article 3. The TSM Regulation recognizes the rights of users to access information on certain aspects related to the net neutrality principle (whether published and/or included in contracts between ISPs and end-users).

To guarantee monitoring to ensure that these rights are respected, and that any infringement thereof is duly penalized, the Regulation grants NRAs the necessary powers to enforce compliance with the Regulation. Moreover, it provides that it is mandatory for consumers to have recourse to mechanisms for resolving disputes concerning matters that are subject to regulation, both in circumstances that involve the operator and in those that do not.

NRA in Spain

As previously mentioned, the essential purpose of the TSM Regulation is:

- "to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights."

- to guarantee the right of end-users "to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service."

The Ministry of Digital Transformation and the Civil Service, and within it SETELECO, is responsible for consumer protection in the electronic communications sector in the terms set forth in Article 99(g) of the GTA.

The Telecommunications Users' Assistance Office (hereinafter, TUAO), attached to SETELECO, is the specific body for the resolution of disputes between end-users of electronic communications services and operators. According to the 2025 annual report published by TUAO,[2] said Office received a total of 12,454 complaints and responded to 32,032 queries during that year.

Period analysed and methodology

This report covers the monitoring activities carried out in 2025.

The results were obtained by:

- Monitoring the electronic communications market

- Requesting information from operators

- Requiring periodic reports from operators to SETELECO (on contracts, offers, modifications, etc.)

[2] https://www.usersteleco.gob.es/quienes-somos/datos-informes.

- Maintaining informal communication with bilateral and multilateral operators

- Analysing queries and complaints received by the TUAO

Principal conclusion

As in prior years, it can be concluded that no significant conflicts arose in 2025 with respect to application of the net neutrality principle as set forth in the TSM Regulation.

The number of complaints received in relation to this issue was of limited significance. As will later be seen, only 2.45% of the complaints received by the TUAO in 2025 can be considered to relate to net neutrality, while 0.32% concerned internet access speed.

As regards the rights recognized in Article 3 of the TSM Regulation, SETELECO analysed the offers placed on the market by operators, determining their compatibility with the aforementioned Regulation and requiring their modification or removal by operators in the event of non-compliance.

Since 2017, major advances have been made with respect to the transparency of the information offered by operators. Most operators have now published the upload and download speeds of the internet access services (IAS) they offer in their contracts, pursuant to Article 4 of the TSM Regulation.

The 2023 *Report from the Commission to the European Parliament and the Council on the implementation of the open internet access provisions of Regulation (EU) 2015/2120*[3] (hereinafter, the 2023 Commission Report) stated the Commission's findings that implementation of the TSM Regulation had been consistent throughout the Union since its entry into force. The findings of the 2025 *BEREC Report on the implementation of the Open Internet Regulation* (hereinafter, the 2025 BEREC Report) are along the same lines.[4]

[3] See APPENDIX III

[4] See APPENDIX III

2. SAFEGUARDING OF OPEN INTERNET ACCESS

Article 3

Safeguarding of open internet access

1. End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service.

This paragraph is without prejudice to Union law, or national law that complies with Union law, related to the lawfulness of the content, applications or services.

2. Agreements between providers of internet access services and end-users on commercial and technical conditions and the characteristics of internet access services such as price, data volumes or speed, and any commercial practices conducted by providers of internet access services, shall not limit the exercise of the rights of end-users laid down in paragraph 1.

3. Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.

The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.

Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:

a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers;

b) preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users;

c) prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

4. Any traffic management measure may entail processing of personal data only if such processing is necessary and proportionate to achieve the objectives set out in paragraph 3. Such processing shall be carried out in accordance with Directive 95/46/EC of the European Parliament and of the Council. Traffic management measures shall also comply with Directive 2002/58/EC of the European Parliament and of the Council.

5. Providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services shall be free to offer services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality.

Providers of electronic communications to the public, including providers of internet access services, may offer or facilitate such services only if the network capacity is sufficient to provide them in addition to any internet access services provided. Such services shall not be usable or offered as a replacement for internet access services, and shall not be to the detriment of the availability or general quality of internet access services for end-users.

2.1 The net neutrality principle

In accordance with the net neutrality principle, ISPs should treat all traffic equally, without discrimination, irrespective of the content or website accessed or the application used. Similarly, they must not apply differentiated treatment based on the type of terminal equipment or method of communication used for access.

Recital 1 of the TSM Regulation provides that the Regulation aims to:

> *establish common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights. It aims to protect end-users and simultaneously to guarantee the continued functioning of the internet ecosystem as an engine of innovation.*

For its part, the Organisation for Economic Co-operation and Development (OECD), in the 2019 OECD Digital Economy Paper *The Effects of Zero Rating* (hereinafter, the 2019 OECD Report)[5] asserts that:

> *Network neutrality, sometimes shortened to 'net neutrality', deals with issues related to non-discriminatory treatment of Internet traffic and the ability of users of the Internet to access content and applications of their choice. The issue can be divided into two broader areas. One deals with factors that affect the ability of users to access content and applications, such as different levels of quality, degradation or blocking of access, or differential pricing. It focuses on the link between the user and the Internet Service Provider (ISP). The second area relates to commercial arrangements between network operators and content providers (CPs).*

In the past it was assumed that electronic communications networks could not unconditionally guarantee a quality of service (QoS) level, and that there were a number of factors that could cause the quality perceived by the user to be inferior to the "maximum" level or the level "advertised" at the time the service was contracted. In this regard, operators usually offer what is referred to as their *"*best effort*"*.

According to BEREC:[6]

> *The best effort internet is about the equal treatment of data traffic being transmitted over the internet, i.e. that the 'best efforts' are made to carry data, no matter what it contains, which application transmits the data ("application-agnosticism"), where it comes from or where it goes. The benefits of the best effort internet notably include the separation between application and network layers of the internet. This separation enables innovation of applications independent of the ISP, thereby enhancing end-user choice.*

The vast majority of the institutions involved recognize that, to a greater or lesser extent, the net neutrality principle must be guaranteed by the pertinent public authority. The principal goal pursued is that of protecting the end-user's right of choice of operator and their right to access and distribute information (and with this their freedom of expression). But implementing the net neutrality principle also entails protecting free competition between

[5] See APPENDIX III

[6] BEREC website, "Net Neutrality" section: https://berec.europa.eu/eng/netneutrality/

ISPs and content providers, and guaranteeing an environment that favours innovation. In this regard, Recital 3 of the TSM Regulation provides as follows:

> *The internet has developed over the past decades as an open platform for innovation with low access barriers for end-users, providers of content, applications and services and providers of internet access services. The existing regulatory framework aims to promote the ability of end-users to access and distribute information or run applications and services of their choice. However, a significant number of end-users are affected by traffic management practices which block or slow down specific applications or services. Those tendencies require common rules at the Union level to ensure the openness of the internet and to avoid fragmentation of the internal market resulting from measures adopted by individual Member States.*

The need for action to be taken by public authorities has also been asserted, as follows, by the *Internet Society*:[7]

> *Discussions about net neutrally, for example, often touch on concerns about freedom of expression, competition of service and user choice, impact on innovation, nondiscriminatory traffic management practices, pricing, and overall business models. From this net neutrality dialog, some believe that policy and regulatory measures are necessary to preserve the open Internet and ensure that it remains an engine for innovation, free expression, and economic growth. The Internet Society believes that focusing on the outcome of network management practices rather than the technical or policy measures employed to deliver that outcome will facilitate necessary flexibility in network operations.*

In the European Union, the response to this need for policy and regulatory measures is the TSM Regulation.

The safeguarding of open internet access provided for in Article 3 of the TSM Regulation is primarily monitored by evaluating the information on offers and price plans that operators are required to send to the NRAs at least one month before they are launched. This analysis is completed by additional monitoring of the information published by operators on their websites. Moreover, SETELECO requires frequent reports from operators on all aspects of their tariffs that could have an impact on net neutrality.

[7] Internet Society website, "Net Neutrality" section:
https://www.internetsociety.org/es/policybriefs/networkneutrality/

2.2 Zero rating offers

'Zero-rating' is when an ISP applies a price of zero to the data traffic associated with a particular application or class of applications (and the data used does not count towards any data cap in place on the internet access service). ISPs have been offering this service at no additional cost for the user.

Paragraph 40a of the 2022 *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules* (hereinafter, the 2022 BEREC Guidelines)[8] confirms the following regarding this practice:

> *Zero tariff options are a subset of differentiated pricing practices which are inadmissible. The ECJ defines zero tariff options as "a commercial practice whereby an internet access provider applies a 'zero tariff', or a tariff that is more advantageous, to all or part of the data traffic associated with an application or category of specific applications, offered by partners of that access provider." Those data are therefore not counted towards the data volume purchased as part of the basic package.*

The above was established in the wake of four rulings —one in September 2020 and three in September of 2021— handed down by the Court of Justice of the European Union on this matter.[9]

In that regard, the 2025 BEREC Report, [10] confirms that, three years on from the rulings, just three countries have reported potential 'zero-rating' commercial tariffs as part of legacy offers, which are in the process of being eliminated.

[8] https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-the-implementation-of-the-open-internet-regulation-0

[9] Judgment of 15 September 2020 regarding the cases C-807/18 and C-39/19
Judgment of 2 September 2021 regarding the case C-854/19
Judgment of 2 September 2021 regarding the case C-5/20
Judgment of 2 September 2021 regarding the case C-34/20

[10] See Appendix III.

SETELECO criteria regarding zero rating offers:

In accordance with the rulings handed down by the CJEU and the BEREC Guidelines on the matter, zero rating offers are no longer admissible.

2.3 Restrictions on the use of equipment

2.3.1 Modem / router provided by the operator

A significant number of operators affirm that, in the case of fixed-network internet access services, users must use a router provided by the operator itself and may not use an alternative router of their own. In principle, this could be considered a restriction on the freedom of choice of terminal equipment recognized in Article 3(1) of the TSM Regulation.

Applicable legislation

The only applicable legislation is the provision contained in the aforementioned Article 3(1) of the TSM Regulation:

> *End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service.*

This Article is complemented by the following three paragraphs from the 2016 BEREC Guidelines on the Implementation of the Open Internet Regulation, which were not significantly amended in the 2022[11] update:

- Paragraph 25. *Thirdly, end-users have the right to use terminal equipment of their choice. Directive 2008/63/EC defines "terminal equipment" as "equipment directly or indirectly connected to the interface of a public telecommunication network". The right to choose terminal equipment therefore covers equipment which connects to the interface of the public telecommunications network. This interface, the network termination point (NTP) 15,*

[11] See Appendix III

is defined in Article 2 (9) of the EECC referring to the physical point at which an end-user is provided with access to a public electronic communications network.

- Paragraph 26. *In considering whether end-users may use the terminal equipment of their choice, NRAs should assess whether an ISP provides equipment for its subscribers and restricts the end-users' ability to replace that equipment with their own equipment, i.e. whether it provides "obligatory equipment".*

- Paragraph 27. *Moreover, NRAs should consider whether there is an objective technological necessity for the obligatory equipment to be considered as part of the ISP network. If there is not, and if the choice of terminal equipment is limited, the practice would be in conflict with the Regulation.*

Analysis of the practice of limiting the use of terminal equipment

The above notwithstanding, it must be determined whether or not this practice does actually limit the use of terminal equipment. In fact, according to the clarification demanded by SETELECO, operators consider basic terminal equipment for internet access to be that used directly by the customer in order to enjoy their internet connection service, i.e., the equipment used to run applications, such as computers (whether desktop or laptop), tablets, televisions or any other equivalent device.

Provision of the internet access service requires the provision and specific configuration of a modem by the operator. This equipment adapts the signal from the equipment (computers, tablets, etc.) used by the customer to access the internet, offering the necessary connection interface to enable interoperability and transmission of the network signal. Modems are configured to synchronize communication with the headend where the operator's internet access servers are located.

Routers serve an additional function. Essentially their purpose is to take the internet connection provided by the modem and split that connection into multiple lines of service for all the different devices used by the customer to access the internet. Consequently, if a customer only connects to the internet using one device, they will usually not have a router because a modem will be sufficient to meet their connectivity needs. Although the functionality of routers is basic and limited, they are important to the internet access experience of individual customers because for many years now they have also offered the possibility of managing connections through the WI-FI interface.

Taking into account the above, it should be clarified that the operator could grant the customer full freedom to choose their basic terminal equipment, meaning there would be no

restriction on the type of computer, tablet or device of any other kind for managing the applications used by the user to access the internet.

To enable the internet access service, the operator installs a modem that manages communication between the terminal equipment of the customer and the network. This equipment has a specific configuration and manages, among other aspects of the internet service, the IP address, the security measures and the specific configuration of the service contracted by the customer. The design of this equipment is tailored to the operator's network. Therefore, it must be considered that, for the purposes of providing the service, the network termination point is after the modem (or optical network terminal [ONT] equipment in the case of fibre to the home [FTTH] networks and cable modems in the case of hybrid fibre-coaxial [HFC] networks). This equipment provides the internet access service, but on HFC and FTTH networks it also manages the additional telephony and television services currently provided on Next Generation Access (NGA) networks with IP technology.

Customers should be offered the functionalities of both a modem and a router in a single piece of equipment. This would benefit them, increasing efficiency by allowing them to plug in just one device instead of two, by saving space, and by offering optimal integrated functionality.

Considering the integration of the functions of both a modem and a router into a single piece of equipment, in principle the initial premise regarding the theoretical impossibility of customers installing their own terminal equipment would be true. However, that premise considered the provision of a single piece of equipment functioning as both a modem and a router, but if the two functionalities were differentiated, nothing would prevent the customer from connecting their own router to manage the entire set of connections and to multiplex the signal.

In this scenario, the customer would connect their own router to the ethernet port of the equipment provided by the operator—of which they would only use the modem functionality—and manage the connectivity of their network of devices independently of the operator. They could enable or disable the router function of the integrated router and modem equipment provided by the operator.

The customer could then connect their own router to manage the internet access to the network equipment provided by the operator. The router could therefore be freely purchased by the customer if they so wished.

Allowing a network configuration of this nature would mean that the modem provided by the operator would be considered to form part of their network and therefore fall under their responsibility.

Situation in other European countries

The BEREC Reports[12] describe the situation in a number of European countries with regard to this problem. The findings of the NRAs in these countries are as follows:

- Cyprus (2021). The NRA's main findings were that most of the ISPs offer their services together with their own terminal equipment in order to provide support and bundled services. The NRA considers this practice to be in accordance with the Regulation.

  End-users, for their part, retain the right, recognized by law, to use their own terminal equipment.

- Finland. The NRA has required ISPs to remove a condition whereby consumers were only allowed to use cable modems that had been pre-approved by the operator.

- Italy (2019, 2020). In August 2018, the NRA published a decision stating that end-users have the right to freely choose their broadband router. According to the NRA, ISPs cannot require end-users to rely exclusively on the router supplied by the ISP itself. This decision was appealed.

  The NRA determined that, due to technological necessity, it was in accordance with the TSM Regulation for ISPs to provide their own modems in order to supply an IAS based on FTTH and FWA solutions. It ruled that operators which offer modems must also provide an alternative offer without modem.

  In April 2021, the NRA fined an ISP for preventing the subscription of FTTH offers that did not include the terminal equipment provided in bundle.

  In the period from December 2021 to February 2022, the NRA conducted an assessment regarding the usage on the networks of two ISPs of the MAP-T and MAP-E protocols and the related compatibility concerns regarding user-provided modem equipment. The NRA concluded that there is enough choice on the modem market to

[12] See APPENDIX III

support these protocols, considering also the fact that the adoption of those protocols will help the transition to IPv6 networks.

2025. As regards discussions or plans to specify the location of the network termination point, in Italy, the NRA has opened a procedure and a public consultation to set the point in fixed networks. The aim is to re-evaluate the current restrictions for FTTH and FWA networks, especially concerning ONTs for FTTH and transceivers for FWA, taking into account technological developments and market changes.

- France (2019). Assessment of the terms and conditions in the mobile market revealed several ISPs' limitations on terminal use. The examination of those cases led to a shift in ISP practices and a consequent modification of offers. On the fixed market, the NRA investigated whether some ISPs were preventing end-users from using other equipment than the standard set-top box.

- Czechia (2021, 2022): The NRA uncovered that ISPs were offering terminal equipment in the form of a lease or purchase. The terms of these contracts included a list of technical parameters that the terminal equipment had to meet, thereby helping end-users to make an informed decision when choosing their own terminal equipment.

  The NRA investigated several cases of suspected restrictions on the free choice of terminal equipment. In one case, the inspection revealed that there was a restriction on the choice and use of the terminal device of one's choice. The provider found to have violated Article 3(1) of the OIR in this manner was fined in joint administrative proceedings.

- Greece (2020): The NRA investigated restrictions placed by some operators on the use of third-party routers.

- Hungary (2020): The NRA considered a clause stipulating that the SIM card associated with the tariff plan could only be inserted into mobile phones to constitute a breach of the TSM Regulation. It also considered a stipulation that certain tariff plans cannot be used for Machine-to-Machine (M2M) communication (e.g. remote monitoring) to be in conflict with said Regulation. Similarly, it considered a clause requiring the SIM card to be used exclusively in the device supplied to the end-user to be in conflict with the legislation.

- Slovakia (2022): All ISPs in the fixed network and some in the mobile network offered their terminal devices for rent or sale but end-users had the option of using their own

terminal equipment based on ISP recommendations to maintain compatibility with the IAS offered. Set-top boxes for Internet Protocol Television were found to usually form part of the supplied TV service.

- Netherlands (2022): In the Netherlands, consumers were found to have full freedom in their choice of terminal equipment. The NRA conducted an investigation into a possible restriction by a cable operator, which resulted in the NRA imposing an order subject to periodic penalty payments on the operator concerned.

- Germany (2022): The NRA detected clauses in contracts offered by four mobile providers that potentially restricted the use of certain terminal equipment under unlimited mobile data tariffs. The NRA formally demanded their amendment and the providers complied.

In the case of Spain, some ISPs appeared to restrict the use of alternative routers to those provided by the ISP. Ultimately, the information provided by the ISPs confirmed that the end-users could use the equipment of their choice.

SETELECO criteria regarding offers analysed that could limit end-users' free choice of router:

Some operators consider it essential to only install routers supplied by them. This practice is not considered to be in conflict with the legislation provided that the end-user may later install a router of their choice. To this end, the operator must provide the end-user with the configuration parameters they request.

2.3.2 Restrictions on the use of connected equipment: tethering

Tethering consists in sharing the data connection on a mobile device with several other devices. This practice entails the use of a smartphone to connect to the general mobile network and to share this connection with other devices through the establishment of a Wi-Fi access point from the smartphone. A small number of offers that restrict this possibility have been detected in Spain.

The BEREC Guidelines (para. 27) consider this practice to fall within the scope of Article 3(1) of the TSM Regulation, and specifically to form part of the right of the end-user to "use terminal equipment of their choice":

> *(27) Moreover, NRAs should consider whether there is an objective technological necessity for the obligatory equipment to be considered as part of the ISP network. If there is not, and if the choice of terminal equipment is limited, the practice would be in conflict with the Regulation. For example, the practice of restricting tethering is likely to constitute a restriction on choice of terminal equipment because ISPs "should not impose restrictions on the use of terminal equipment connecting to the network in addition to those imposed by manufacturers or distributors of terminal equipment in accordance with Union law" (Recital 5).*

As can be seen, this paragraph of the Guidelines, which was not modified in the 2022 revision, is not conclusive, as it claims that this practice is "likely" to constitute a restriction on choice of terminal equipment, referring in turn to Recital 5 of the TSM Regulation, which stipulates that "*providers of internet access services should not impose restrictions on the use of terminal equipment connecting to the network in addition to those imposed by manufacturers or distributors of terminal equipment in accordance with Union law.*"

The aforementioned Recital appears instead to refer to a possible restriction on the type of device rather than the number of devices used. Operators claim that a lack of restrictions in this regard could lead to multiple users making use of a single data connection. In fact, the few offers found to restrict tethering were also zero rating offers.

This last detail is important, given that the tariff dynamic in this market could lead to a proliferation of offers that include limitations on tethering. The increase in the number of "infinite" or "unlimited" mobile data plans could cause operators to impose restrictions on tethering in the guise of "fair use polices" in the same way that limitations have been imposed on other services such as roaming or even voice calls in unlimited data plans.

Situation in other European countries

To date, few decisions have been made within the EU in relation to the practice of limiting tethering. The BEREC Reports[13] describe the situation in this regard in a number of European countries:

- Norway (2019, 2020): The NRA considered the ban on tethering imposed by the ISP, and its decision not to offer SIM cards that could be inserted into end-users' own routers to be in conflict with the Regulation.
- Germany (2019, 2020, 2021, 2022). A consumer association sued Vodafone over various clauses in the terms and conditions of Vodafone Pass, a purportedly zero rating offer in which data consumed by tethering (as well as by voice- and video telephony) was nonetheless counted against the data allowance. The court dismissed the claim on the grounds that the contract did not prohibit tethering.[14]
- Greece (2021). A case was investigated regarding terms restricting tethering in subscriber contracts. The ISPs responded that no limitations were placed on tethering in practice and the only restrictions concerned data sharing between different SIM cards. The terms were clarified and the case was concluded.

In the case of Spain, operators confirm that there are currently no tethering restrictions in place.

SETELECO criteria regarding offers analysed that limit data sharing with devices not directly connected to the network (tethering):

Offers that could limit data sharing with devices not directly connected to the network have been considered to be in conflict with the TSM Regulation. Such restrictions would only be admissible if used as temporary and exceptional traffic management measures for tackling network congestion.

[13] See APPENDIX III

[14] *"…The court argued that counting data consumed by tethering against the data allowance does not constitute a violation of Article 3(1). The main reason for this was that tethering is not contractually forbidden." (p. 51 of 2020 report)*

2.3.3 Restrictions on the use of multi-SIM cards

The proliferation of unlimited mobile data plans has led to a tendency among operators to place restrictions on certain practices and terms of contract. In addition to tethering (see above), some operators place restrictions on or opt not to offer the multi-SIM service in the case of unlimited mobile data plans.

The multi-SIM service consists in the provision of additional or supplementary SIM cards associated with the same mobile line as the user's main card, for use on devices other than the main device with which the main SIM card is associated (such as PCs, tablets, smartwatches). These supplementary cards can be physical or embedded SIM cards.[15]

This option does not pose any particular problems for operators in limited data plans, as the total volume of data would constitute the download limit for the sum of all the devices used.

However, the maintenance of this service in unlimited plans could lead, in practice, to one line effectively functioning as two or more lines with unlimited data, given that they would be being used in this way for each device in which the supplementary card was inserted.

Current regulation

Neither the TSM Regulation nor the 2022 BEREC Guidelines include any provision regarding this specific problem, beyond the following clause of Article 3(1) of the Regulation:

> *End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service.*

Moreover, the BEREC Reports on the implementation of the Regulation do not contain any specific references to this problem either.

[15] An eSIM, virtual SIM or virtual card is embedded in the hardware of the mobile phone, tablet or smartwatch itself. This removes the need to physically insert the card or replace it with a new one in the event of changing operator.

Practices in Spain

- Establishment of two modalities for contracting the multi-SIM service associated with a specific plan: a more economical service with lower mobile data download speed when using supplementary cards; a costlier service without any such restrictions

- Provision of service without any type of restriction by some operators

- Verification of the existence of unlimited data offers that place caps on mobile data consumption

SETELECO criteria regarding multi-SIM card offers:

In limited mobile data plans, there are no grounds for restricting the use of multi-SIM cards. Any restriction would be considered to be in violation of the TSM Regulation.

In unlimited data plans, it is admissible for ISPs to impose restrictions for the purpose of preventing users from converting one line into multiple lines by linking a different card to each device. However, the data consumptions of each secondary device used should be treated equally.

2.3.4 Restrictions on the use of SIM cards

The freedom of choice regarding terminal equipment provided for in the TSM Regulation encompasses the option of using or inserting the mobile line SIM card in any device. Neither the TSM Regulation nor the BEREC GUIDELINES expressly examine this specific right, which implicitly stems from the right to freedom of choice regarding terminal equipment.

Actions in 2025

As in prior years, an analysis has been conducted of the conditions established by operators in this regard. It has been verified that the ban on using SIM cards in devices other than mobile phones refers exclusively to their insertion in devices aimed at provoking irregular traffic or reselling traffic (SIM box).

SETELECO criteria regarding offers analysed that restrict the use of SIM cards in certain devices:

Offers limiting the use of SIM cards in certain devices have been considered to be in conflict with the TSM Regulation. Such limitations are only admissible in the case of devices used to resell telephone traffic or to produce irregular or undue traffic.

2.4 Traffic management measures

Article 3(3) of the TSM Regulation lays down the general principle of equal treatment of all traffic by the operator.

> *Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.*

The subsequent subparagraphs of that Article develop this principle while at the same time providing for certain exceptions to its application, in defence of interests such as the integrity and security of the network and compliance with orders by courts or public authorities.

In this regard, the 2019 OECD Zero Rating Report[16] states that:

> *As a starting point, it is important to note that the principal idea behind net neutrality is equal treatment of all data traffic –* ***a bit is a bit, irrespective of its content, its origin or destination****.*

The aforementioned OECD report goes on to concede that basic traffic management is admissible in some instances, even if it requires different treatment of different categories of services (for example, for reasons of urgency): "This may justify qualitative differences in treatment of whole classes of data and prioritising real-time services (like voice)." It also refers to the fact that in the European Union, the regulation of net neutrality "allows for such

[16] See APPENDIX III

different traffic management measures if they are based on objectively different technical Quality-of-Service requirements".

The Internet Society[17] warns against the possible use of traffic management measures to serve interests or aims other than those provided for in the legislation. This is one of the core aspects of the net neutrality principle. It highlights that some network operators must use congestion-management and traffic-shaping techniques to keep their networks running smoothly. Consequently, there are those who worry that network operators are technically able to use traffic-management practices to give preferential treatment to certain data streams. Others are concerned that practices adopted to increase revenues might block competing content or offer unfair advantage to some content over others. They see these practices as problematic, especially when they intentionally discriminate against certain kinds of content delivery to the detriment of end-users. This has led to greater public concern that these kinds of practices jeopardize the principles of openness and transparency of the internet.

A key element of internet architecture is that user data is relayed across the internet in the form of standardized packets of information, irrespective of their content, sender, or recipient. This non-discriminatory approach to internet traffic is a central premise of the functioning of the internet. It allows data to flow easily across networks without encountering obstructions caused by its own nature. Essentially, this open internet working approach is one of the pillars sustaining the internet and key to its success.

In practice, however, data packets are sometimes treated differently in order to address network congestion, resource constraints, business arrangements and other practical considerations concerning the functioning of the network. Some network providers argue that current bandwidth and infrastructure resources are congested and that significant network-management intervention is required to solve this problem and to offer a good quality of service to customers. Whether these network management practices constitute fair and impartial treatment of the data that travel across the internet is a matter of some debate. There are also questions as to what extent network management activities could constitute discriminatory practices, potentially restricting access to content and limiting internet users' freedom of expression.

[17] https://www.internetsociety.org/es/policybriefs/networkneutrality/

2.4.1 Traffic management measures executing court rulings

Regulation

Article 3.3 of the TSM Regulation states that:

> *"Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:*
>
> *(a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers;"*

In addition, Article 76.3.a) of the GTA stipulates that:

> *"Internet access service operators shall not engage in traffic management measures going beyond those set out in the preceding paragraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:*
>
> *(a) comply with European Union law or national law to which the internet access service operator is subject, or to fulfil court judgments;"*

<u>Judgment No. 310/2024 of 18 December 2024, of Commercial Court No. 6 of Barcelona.</u>

The judgment was handed down to protect usage rights for the audio-visual content from Campeonato Nacional de Liga (National League Championship) First Division and Second Division football matches in Spain.

Those rights are protected by law in the closing paragraph of Article 138 and by Article 139.1.h) of the Consolidated Text of the Intellectual Property Act,[18] and by the interpretation of those provisions by Section 15 of the Provincial Court of Barcelona in its judgment of 20 February 2018, by Commercial Court No. 6 of Barcelona in its judgment of 12 January 2018, by

[18] https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930.

Commercial Court No. 2 of Barcelona in its judgment of 25 June 2016, and by the Court of Justice of the European Union in its judgment of 27 March 2014 in the UPC Telekabel case. All of the cited judgments favoured allowing intellectual property rights-holders to take action directly against information service providers.

Judgment 310/2024 of Barcelona Commercial Court No. 6 orders an immediate blocking of IP addresses that were used to illegally distribute LA LIGA content and future blocks on access. In that regard, the court also ordered that the specific blocked IP addresses be monitored for a limited period (to be counted by sporting seasons), in order to identify any substitute IP addresses.

In response to the ordered IP bans, a number of appeals were lodged against the judgment, requesting that it be annulled. The appeals were dismissed (Order No. 295/2025 of 25 March 2025).

The cited order dismisses the argument that the procedure is one of indiscriminate blocking, and specifically states that there are not "insufficient guarantees". In the order, the court also stated that it "did not find, based on the arguments put forward by the various appellants, that any harm has been caused, not is any harm identified or quantified, and no request is made to gather evidence to demonstrate that harm has been caused directly or indirectly as a constituent component of the appellants' claims".

It was therefore found that the disagreements concerning IP blocking implemented in enforcement of the judgment must be addressed and ruled on in the context of fulfilment and enforcement of court judgments.

2.4.2 Traffic management measures and 5G technology

The launch of 5G mobile technology and its potential for facilitating different treatment of traffic by category is problematic from a net neutrality perspective, as it increases the likelihood that operators will introduce traffic management measures. However, the operators themselves are concerned that an excessively rigid regulation of this matter could hamper the appearance of new services and, with it, technological innovation.

5G technology and network architecture

a) **Network slicing.** This is a technique that creates multiple virtual networks on top of a shared physical network. Each network slice is an isolated end-to-end network tailored to

meet the diverse requirements needed by a particular application. In this way, it is possible for different slices to offer different services within the same network.

b) ***5G QoS Class Identifier* (5QI).** 5QI is a mechanism in which packets are classified into different QoS classes. In this way, the QoS can be tailored to specific requirements. Each QoS class has its own assigned characteristics (such as packet delay and packet loss). As a result, some packets can obtain better QoS than other packets.

c) **Mobile Edge Computing (MEC).** Also known as Multi-access Edge Computing,[19] MEC is a network architecture that enables cloud computing to be performed at the edge of a mobile network, i.e., at a location close to the base station. Currently, many applications carry out their online computations and content storage on servers at a considerable distance from devices and end-users. MEC brings these processes closer to the user by integrating them with the local cellular base stations.

Draft Further Guidance on 5G Network Slicing. Annex to the BEREC Guidelines.[20]

BEREC recently published a document for public consultation, to complement the current Guidelines, which once adopted will provide additional guidance for operators to self-assess the compliance of the 5G network slicing services they offer with net neutrality regulations.

This follows on from the 2023 Commission Report, which among other findings, stated that some operators considered that *"the current rules and approach do not provide sufficient certainty to enable them to launch services based on network slicing or define specialised services"* and that *"[g]reater legal certainty could therefore be beneficial to both innovators and consumers in the future".*

Although the guidance focuses specifically on 5G network slicing services, its underlying principles are considered to be applicable for future 6G architecture. Given the underlying principle of technological neutrality of the TSM Regulation, the approach set out is equally important for similar QoS differentiation mechanisms in other network technologies. In the event of a conflict between the Guidelines and the Appendix, the Guidelines shall take preference.

5G network slicing services must be analysed according to the general rules on neutrality contained in the Regulation and are subject to the general obligation to treat all traffic

[19] https://www.magazcitum.com.mx/index.php/archivos/5218.
[20] https://www.berec.europa.eu/en/all-documents/berec/regulatory-best-practices/guidelines/draft-further-guidance-on-5g-network-slicing.

equally pursuant to Article 3(3)- Reasonable traffic management measures may be implemented provided that they are not based on commercial considerations.

Pursuant to Article 3(2), different QoS and individual commercial conditions may be offered, provided that they are transparent and "application-agnostic". Provision of services with a better QoS level should not degrade the quality of the other services.

Lastly, the guidance offers eight examples of services and corresponding assessments of their permissibility under the legislation.

2.4.3 Reasonable traffic management measures

The second subparagraph of Article 3(3) of the TSM Regulation provides as follows:

> *The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.*

In accordance with this provision, operators may adopt traffic management measures that are "reasonable". To this end, they must meet the following requirements:

- They must be "transparent, non-discriminatory and proportionate".
- They should not be based on commercial considerations, but on "objectively different technical quality of service requirements of specific categories of traffic".
- Such measures shall not monitor specific content.
- And lastly, such measures should not be maintained for longer than necessary.

From the outset certain practices have been identified that would meet these requirements.

a) <u>Differentiating quality of service</u>

According to the 2018 BEREC Opinion,[21] offering different internet speeds on mobile networks at different prices is permissible under the Regulation, as are contractual modalities that offer different latency, jitter and packet loss parameters. Moreover, in this same Opinion, BEREC affirms that:

> *The question whether offering different IAS subscriptions with different non-discriminatory QoS classes would be allowed, for example to implement different speeds for different mobile IAS subscriptions, has been raised by multiple stakeholders. BEREC understands this to be both current practice, and compatible with the Regulation as long as the practice does not limit the exercise of the rights of end-users.*
>
> *[…]*
>
> *It is reasonable to conclude that further QoS parameters, other than data volumes and speeds, such as latency, jitter and packet loss, could be agreed upon. Therefore, it would be permissible for the ISP to provide different QoS classes based on combinations of the above QoS parameters for different IAS subscriptions where the QoS classes are application-agnostic and transparency is ensured – as long as the practice does not limit the exercise of the rights of end-users.*
>
> *[…]*
>
> *Furthermore, the Regulation does not prevent end-users from buying more than one subscription with different QoS classes, and using them as they want for different applications.*

The 2019 Commission Report[22] expands upon this idea, considering that the offer of different QoS modalities is legally possible provided that transparency is guaranteed. Despite the existence of factors that can result in two users experiencing different QoS levels (such as the terminal equipment used or the content accessed), they are considered as being treated equally if traffic management measures are based on objective technical justifications that benefit the overall quality and/or efficiency of the network.

For its part, the 2023 Commission Report concludes that:

[21] See APPENDIX III

[22] See APPENDIX III

The QoS levels should remain 'application agnostic' while the end-users should remain in control over which applications are transmitted over which QoS level.

In this regard, the 2018 BEREC Opinion establishes the following:

- *There is a limitation to the implementation of different QoS classes in the sense that an ISP cannot provide some end-users premium IAS subscriptions to such an extent that it degrades the quality to other IAS subscriptions to a quality below the contract conditions agreed under Article 4(1) or the minimum level of quality that may be defined according to article 5(1) of the Regulation.*
- *[W]hen IAS subscriptions with different QoS classes are provided during temporary network congestion, any reduction of the quality should be proportionate to the agreed quality of the different QoS classes.*

b) <u>Compression or throttling of traffic</u>

Any traffic management measure tending to decrease speed, resolution or transmission rate could be included under this heading. Normally such measures are applied to video streaming content.

In principle this type of practice is prohibited by the third subparagraph of Article 3(3) of the TSM Regulation, which provides for it only under exceptional circumstances of limited duration:

> *Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:*
>
> *(a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers;*

(b) preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users;

(c) prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

Under all other circumstances, "slowing down", "degrading" or "restricting" specific content, applications or services, or specific categories of content, applications or services, would be prohibited. However, as clarified in Recital 11 of the TSM Regulation:

Rules against altering content, applications or services refer to a modification of the content of the communication, but do not ban non-discriminatory data compression techniques which reduce the size of a data file without any modification of the content. Such compression enables a more efficient use of scarce resources and serves the end-users' interests by reducing data volumes, increasing speed and enhancing the experience of using the content, applications or services concerned.

In this regard, the 2018 BEREC Opinion,[23] seeks to clarify the distinction between data compression and throttling:

According to Recital 11, the Regulation does not ban non-discriminatory data compression techniques that reduce the size of a data file without any modification of the content. Lossless compression (i.e. original data can be reconstructed exactly from the compressed data) would therefore be in line with the traffic management rules under the Regulation.

However, BEREC considers that throttling by the ISP of any data stream within the IAS, such as for example video traffic, is not in line with Article 3(3) first sentence, as "restriction or interference" of the traffic on the IAS is not allowed. By analogy, BEREC also considers it not allowable to use such application-specific throttling to force a CAP to supply video content in a lower resolution by the use of adaptive bitrate coding. Such practices would not represent data compression according to Recital 11.

Operators' position

[23] See APPENDIX III

Operators, in response to SETELECO information requirements, have clarified that, once identified, video traffic passes through the video optimizer, which applies adaptive bitrate (ABR) techniques. Through the use of ABR, adjustments are made to video quality and image resolution.

Making use of adaptive bitrate streaming (used by most video content providers) allows video content to be downloaded more efficiently, minimizing poor user experience in the event of network congestion. In this way, the limited resources of the mobile network are distributed more efficiently, providing a better customer experience by maintaining continued, uninterrupted viewing, even though the network may reach a certain level of saturation.

The ABR mechanism, which prevents customers from accessing maximum video quality levels that are indistinguishable on a mobile screen from lower quality levels, is capable of providing a consistent user experience.

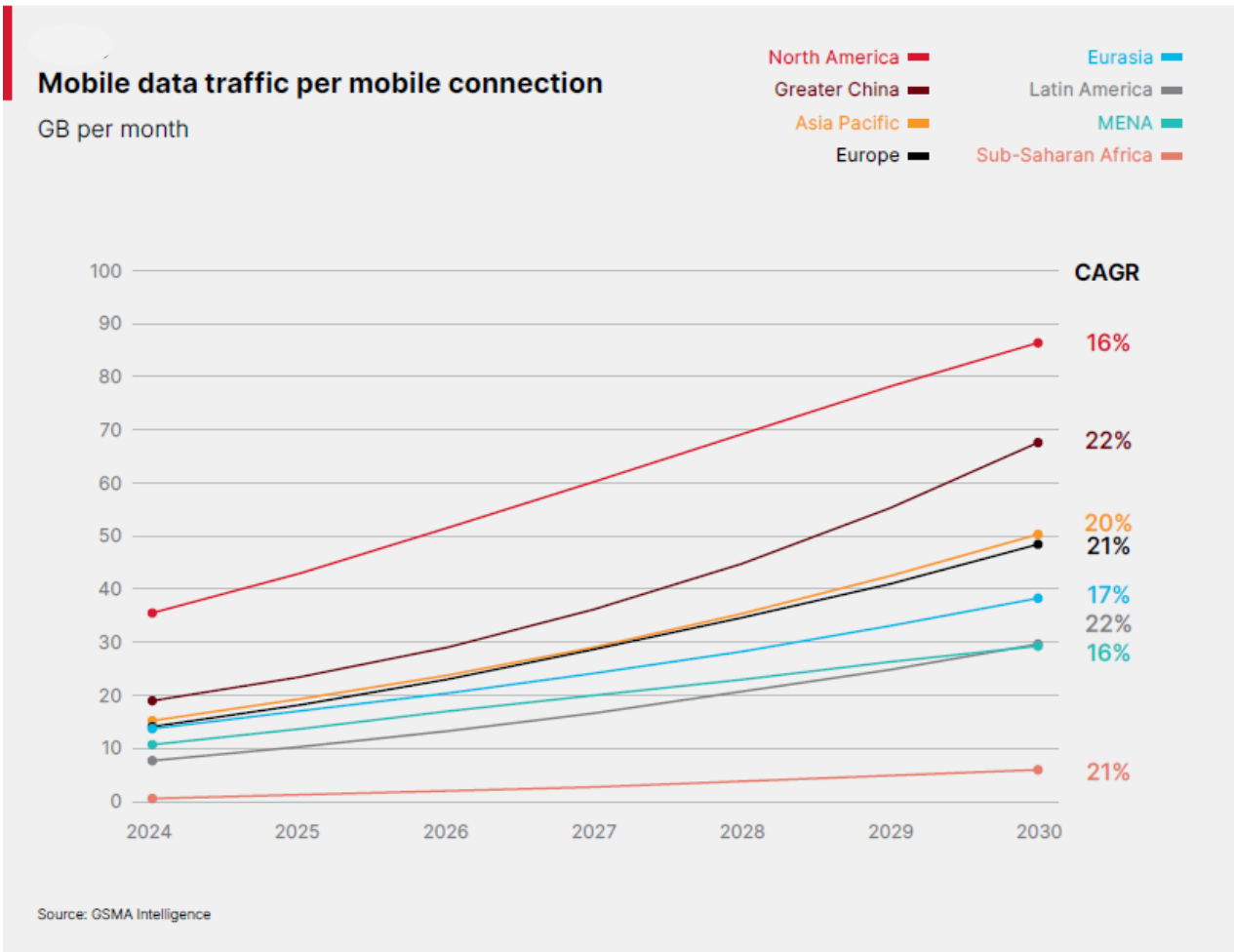
This mechanism is based on adapting the video streaming QoS based on the available information stored in the database of the Global System for Mobile Association (GSMA) about the resolution capacity of the terminal equipment. Depending on its capacity, each terminal is associated with the most appropriate QoS so that ABR services can make the most efficient use possible of the bandwidth.

These video streaming optimization measures do not differentiate between content and video providers, but only determine whether they meet the capacity criterion of the terminal used, i.e. they adapt the streaming speed of the video depending on the device (resolution) that the customer is using to view that content, making no distinction on the basis of tariff or content provider and without affecting customer experience.

Therefore, this measure, in addition to preserving network integrity, optimizes the consumption of the data packet contracted by customers by offering qualities adapted to the capacity/resolution of the terminal used.

Operators insist on the need for this practice, which is especially pressing given the expected increase in data use on mobile networks. According to the GSMA[24] report *"The Mobile Economy 2025"*, current predictions are of a 21% increase in average consumption per customer in Europe from 2024 to 2030.

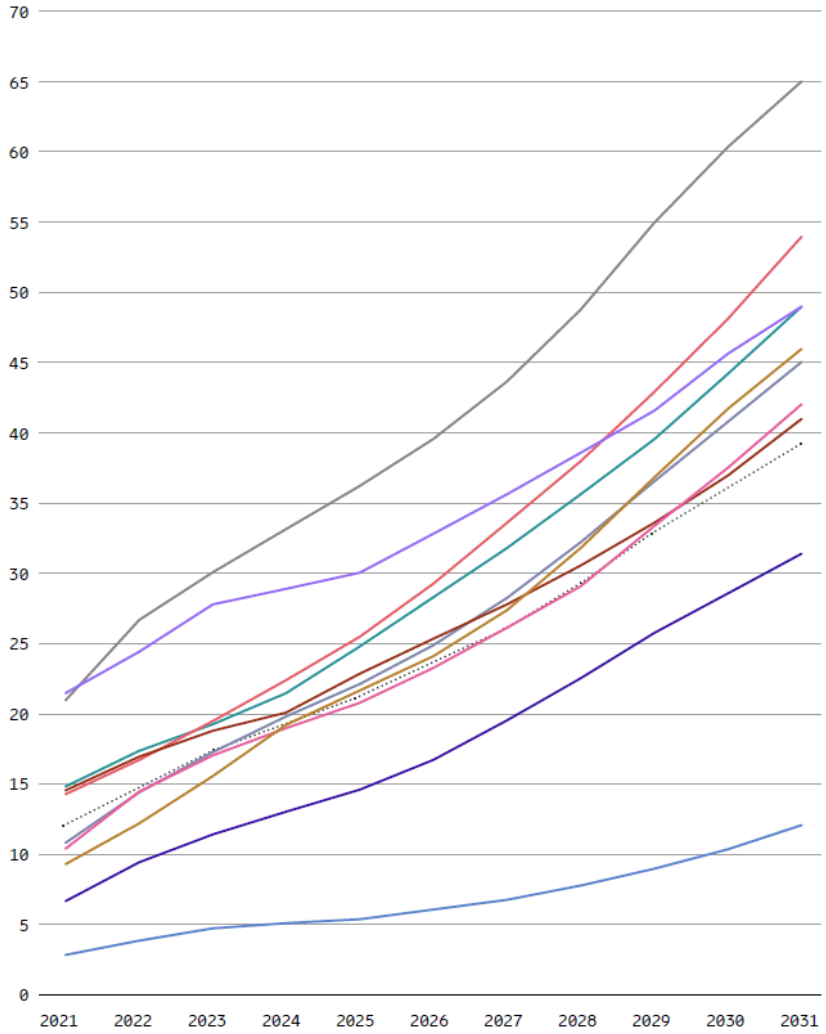
[24] https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2026/01/The-Mobile-Economy-2025.pdf (p.14).



Similarly, according to the Ericsson Mobility Report of November 2025,[25] in Western Europe traffic usage per smartphone is projected to reach 54 GB/month in 2030, compared to 49 GB/month expected usage in North America the same year.

[25] https://www.ericsson.com/4aca6f/assets/local/reports-papers/mobility-report/documents/2025/ericsson-mobility-report-november-2025.pdf (p. 14).

Figure 12: Mobile data traffic per active smartphone[1] (GB per month)



Regions	2025	2031	CAGR 2025–2031
India, Nepal and Bhutan	36	65	10%
Western Europe	25	54	13%
North America	25	49	12%
Gulf Cooperation Council	30	49	8%
Middle East and North Africa[2]	21	46	14%
Central and Eastern Europe	22	45	13%
South East Asia and Oceania	21	42	12%
North East Asia	23	41	10%
Global average	21	39	11%
Latin America	14	31	14%
Sub-Saharan Africa	5	12	15%

1 Traffic per active smartphone refers to all traffic generated by that device, regardless of number of subscriptions attached.

The 2022 BEREC Guidelines

The Public Consultation on the draft BEREC Guidelines on the Implementation of the Open Internet Regulation of 10 October 2019 (hereinafter, the 2019 BEREC Public Consultation)[26] makes specific reference to data compression and throttling. Aware that Recital 11 could result in operators introducing such measures—considering them to fall under the category of "data

[26] See APPENDIX III

compression techniques", which are permitted by this Recital—BEREC proposed the following change to paragraph 77 of the Guidelines:

- *Overall description of the change: ISPs may implement data compression techniques as long as they are lossless i.e. the content originally sent reaches its destination unmodified. Forcing adaptive bitrate coding does not represent data compression according to Recital 11.*

- *Explanation: Some stakeholders argued that application-specific throttling which forces content providers to supply video content at a lower resolution by adaptive bitrate coding represents a form of data compression.*

Pursuant to the new paragraph 77a:

> *ISPs may use non-discriminatory data compression techniques in their networks as long as the content originally sent by an end point reaches its destination end point(s) unmodified, i.e. lossless compression. The use of application-specific throttling e.g. to force a CAP to supply video content in a lower resolution by the use of adaptive bitrate coding does not represent data compression according to Recital 11.*

As set forth above, this new paragraph 77a of the BEREC Guidelines bases the criteria for permissibility on the following two prerequisites:

- That any technique used be non-discriminatory.

- That the content transmitted sent cannot be modified. In this regard, adaptive bitrate encoding is considered to modify content, by forcing content and application providers to supply video content in a lower resolution.

Situation in other European countries

The BEREC Reports[27] identify the following actions:

- Greece considered the practice of throttling video streaming on mobile networks to be in conflict with the Regulation.

Actions in 2025

[27] See APPENDIX III

In prior years two operators were investigated to determine whether the practice of using a file compression system was in line with the new paragraph 77a of the 2020 BEREC Guidelines. The operators confirmed that they had abandoned this practice.

However, monitoring for this practice has been continued.

SETELECO criteria regarding offers that include traffic compression techniques:

The new BEREC Guidelines largely restrict the possibility of using image compression techniques such as ABR.

c) Blocking of content managed by the user

In this respect, the 2019 Commission Report refers to possible future offers, proposed by ISPs at a stakeholder workshop, in which connected objects may connect only to their producer's application and where the end-user may wish to restrict the possibility of connection only to their own devices. The Commission offers the following analysis:

> *A typical example would be a person buying a burglar alarm or a webcam and restricting the devices that are authorised to configure it to those of the premises' inhabitants. In such a case, the internet service provider would implement the access restrictions in the network, but at the request of the end-user. In this case, the choice given to the end-user by Article 3(2) to agree on technical conditions with the internet service provider is relevant. In such a scenario, the obligations in Article 3(3) that apply to the operator blocking end-points do not apply to cases where the end-user is fully in control of –— and establishes item by item — what is blocked or not (and the other technical or commercial conditions of the internet access service do not vary depending on their choice.) However, such practices should be closely monitored in order to ensure that no such choice is imposed by the internet service provider. On the contrary, it should remain under the permanent control of the end-user with easy initial opt-in and subsequent opt-out.*

As can be seen, the key to determining whether or not content blocking is permissible under the TSM Regulation is to identify which party (user or operator) is doing it. In this section we are referring to content blocking by the user, as opposed to blocking carried out to comply with the law, such as blocking of illegal content, court-ordered blocking, blocking to preserve the integrity and security of the network, and blocking to prevent network congestion pursuant to letters (a), (b) and (c) of Article 3(3).

The 2018 BEREC Opinion[28] also includes the following statements in this regard.

- *[T]he scope of the Regulation does not cover software installed at the endpoints, i.e. on terminal equipment such as computers and mobile phones. [...] Therefore, software that is installed on end-users' terminal equipment connected to the IAS could for example enforce parental controls in line with the Regulation.*

- *[T]he Regulation covers the internet access service ("network layer"), but not content and applications (sometimes referred to as "over-the-top") that are transmitted over the IAS. […] In case an email server is filtering spam, this would not be within the scope of the Regulation, since the application servers (in this example the email servers) are endpoints connected to the internet. Therefore this would be permissible.*

- *[F]iltering web content in the network would not be permissible. This is the case when packets are sent between the web server and the web client, and a middlebox inside the network of an ISP (i.e. a middlebox that is not the intended endpoint of the application) may inspect the packets as they are passing, and may manipulate the payload (e.g. by changing ads).*

In relation to the first of these points, an amendment introduced in the 2020 BEREC Guidelines allows for ISPs to offer endpoint-based services such as parental control functions, meaning that pursuant to the BEREC Guidelines themselves, these practices should be evaluated:

> *However, as described in paragraph 32a, ISPs can also offer these end point-based services (e.g. to provide parental control or filtering functions alongside the IAS) in the same way that they are offered by third party CAPs. […] On a case-by-case basis, end point-based traffic restrictions, such as blocking, should be evaluated under Article 3(2) as described in paragraph 32a and further.*

The BEREC Reports identify certain practices adopted by EU Member States:

- Germany (2020): The NRA affirmed that it was investigating the use of parental control filters that blocked websites or downloads. The NRA considers offers that include parental control filters to be permissible under the following conditions: "a) the underlying internet access service must be application agnostic without blockings or other traffic management measure; b) the end-user has to be in full control of the

[28] See APPENDIX III

filtering functions (i.e. by activating or deactivating these functions); c) activating or deactivating must not affect the price (or other conditions) of the IAS."

- Slovakia (2023): Legislation on gambling and on the protection of privacy and of children has been enacted to allow the blocking of inappropriate content. The list of prohibited websites is published by the competent authority.

2.4.4 Traffic management measures for network integrity and security

Regulation

Pursuant to Article 3(3) of the TSM Regulation:

> *Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:*
>
> *a) […]*
>
> *b) preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users;*
>
> *c) […]*

The stipulated pre-requisites, therefore, for the adoption of measures to guarantee network integrity and security are, firstly, that they be necessary, and, secondly, that they only be implemented for as long as they are required. Consequently, measures may not be kept in place indefinitely, unless so provided elsewhere in the Regulation.

For its part, Recital 14 of the Regulation underscores the need for traffic management measures to be adopted to prevent security incidents:

> *Second, traffic management measures going beyond such reasonable traffic management measures might be necessary to protect the integrity and security of the network, for example by preventing cyber-attacks that occur through the spread of malicious software or identity theft of end-users that occurs as a result of spyware.*

Subsequently, this issue has been addressed in several paragraphs of the BEREC Guidelines.[29] Specifically, paragraphs 83 to 87 provide examples of typical attacks and threats that could jeopardize the integrity of the network, including:

- *flooding network components or terminal equipment with traffic to destabilise them (e.g. Denial of service attack);*
- *spoofing IP addresses in order to mimic network devices or allow for unauthorised communication;*
- *hacking attacks against network components or terminal equipment;*
- *distribution of malicious software, viruses etc.*

According to the Guidelines, the measures adopted could include restricting connectivity or blocking traffic to and from specific end points (blocking IP addresses or certain ports). To this end, the use of security monitoring systems by ISPs to identify threats may be justified, even on a permanent basis. Threats can also be identified from users' complaints. Given that the scope of this exception is broad, NRAs must monitor the grounds put forward to justify its application.

In the revision of the 2020 Guidelines, BEREC has amended paragraph 85 to better distinguish between monitoring measures adopted to detect threats and reactive measures put in place to mitigate the impact of threats that have materialized:

> *NRAs should consider that, in order to identify attacks and activate security measures, the use of security monitoring systems by ISPs is often justified. Such traffic management systems consist of two separate components: one component that executes the traffic management itself and one component that monitors traffic on an ongoing basis and triggers the traffic management. Monitoring of traffic to detect security threats may be implemented in the background on a continuous basis. Traffic management measures (such as those listed in paragraph 84) preserving integrity and security are only triggered when concrete security threats are detected. Therefore, the precondition "only for as long as necessary" does not preclude implementation of such monitoring of the integrity and security of the network.*

[29] See APPENDIX III

Moreover, the new paragraph 87 includes an explicit reference to the Guideline of the **European Union Agency for Cybersecurity** (formerly, the European Network and Information Security Agency) (ENISA).

ENISA Guideline

In December 2018, ENISA published its *Guideline on assessing security measures in the context of Article 3(3) of the Open Internet regulation,*[30] which offers specific advice regarding application of the exception provided for in said provision.

The Guideline lists a number of factors to be taken into account by NRAs when evaluating whether or not a security measure is required. These factors and the questions to be asked in their regard are as follows:

a) Security risk

- How severe and urgent is the security threat?
- What is the potential impact of the security threat?
- What is the likelihood that the security threat materializes and has an impact?

b) Effectiveness

- To what extent is the risk mitigated when the security measure is implemented?
- What would the impact be on the network, services and customers if the measure is not applied?
- What is the residual risk?

c) Proportionality

- Is the scope of the measure limited to specific traffic, networks, or end-user?
- What is the duration, is the measure time-limited?
- Is there impact on 'good' network traffic and legitimate services (false positives)?
- Is there impact for the end-users?

[30] See APPENDIX III GUIDELINES ENISA 2018

d) Appropriateness

- Is the measure considered the appropriate measure to mitigate this threat/risk?
- Is the measure recommended in industry good practices or standards?
- Are there alternatives that are more effective or more proportionate?

Application in other European countries

As regards application in other European countries, according to the BEREC Reports,[31] numerous countries have detected port blocking by ISPs aimed at preventing security threats. Almost none of the NRAs have introduced any impediments to the use of this measure.

However, according to the 2020 BEREC Report,[32] ISPs in France may have been required to abandon certain port-blocking practices,[33] after end-users reported that some services or applications were not reachable.

In 2025 the following countries monitored this practice:

- Austria
- Croatia
- Greece
- Malta
- Netherlands
- Poland
- Slovakia

[31] See APPENDIX III

[32] See APPENDIX III

[33] *In addition, end-users also reported that some services or applications were not reachable because of potential port blocking practices from one ISP. Arcep opened an informal dialogue with the concerned ISP, which revealed that the issues were caused by a legacy system implemented in the ISP's network. After identifying the problem, the ISP is taking action to remove this blocking.* 2020 BEREC Report, page 17.

Practices analysed

Only two practices have been detected as a result of the investigations conducted and information requirements imposed in our country. The first of these practices is port 25 blocking. The reason given by operators for implementing this measure is to block spam.

Operators explain that spam can be understood as any kind of unsolicited mail that looks like advertising, but could contain hidden malware and thus represent a security risk for the customer. In extreme cases it could also represent a security risk for the network. Moreover, spam, which accounts for a significant volume of internet traffic, consumes major network resources as well as end-user resources. In addition, its proliferation can be seriously harmful to end-users in those cases where it fills up their inboxes, preventing them from receiving important or necessary mails, or when it is linked to malware incidents.

In this context, taking account of the risks for both the network and users, some operators have decided to filter port 25. Thus, in some cases involving spam and the potential malware associated with it, they have blocked outbound traffic from users towards port 25 on external mail servers. This filter is applied at network level. In addition, they assert that this type of connection is usually made by email servers, but also by malware used to send spam.

Spanish operators also point out that the adoption of traffic management measures such as port blocking to guarantee network integrity and security as well as the services provided on their networks is permitted under the TSM Regulation (Article 3(3)b) and included in the BEREC Guidelines. Similarly, they state that they have the general obligation, in accordance with Article 63 of the GTA, to manage the integrity and security of their networks and services.

Finally, they highlight that this practice has always responded to freedom of choice and arrangements between users and operators (Article 3(1) and 3(2) of the Regulation), given that when a customer is negatively affected by this blocking, for example, because they run their own email server at home, they can ask the operator to unblock it.

The second practice identified is the restriction of traffic upon detection of Distributed Denial of Service (DDoS) attacks: when a DDoS attack is detected, traffic is redirected to equipment that blocks illicit traffic and only allows lawful traffic to pass.

No significant developments were identified in this regard in 2025.

SETELECO criteria regarding offers that include port blocking for security reasons:

SETELECO considers that these offers, and the practice of port blocking for security reasons, i.e. to prevent spam or malware, are in line with the TSM Regulation.

2.4.5 Traffic management measures for network congestion

Regulation

Article 3(3) of the TSM Regulation stipulates that:

Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:

[…]

(c) prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

This Regulation dedicates its extensive Recital 15 to this exception. We wish to highlight the following aspects:

- *The principle of proportionality requires that traffic management measures based on that exception treat equivalent categories of traffic equally.*
- *Temporary congestion should be understood as referring to specific situations of short duration, where a sudden increase in the number of users in addition to the regular users, or a sudden increase in demand for specific content, applications or services, may overflow the transmission capacity of some elements of the network and make the rest of the network less reactive.*
- *Temporary congestion might occur especially in mobile networks, which are subject to more variable conditions, such as physical obstructions, lower indoor coverage, or a variable number of active users with changing location.*

- *Possible causes of those situations include a technical failure such as a service outage due to broken cables or other infrastructure elements, unexpected changes in routing of traffic or large increases in network traffic due to emergency or other situations beyond the control of providers of internet access services.*

- *The need to apply traffic management measures going beyond the reasonable traffic management measures in order to prevent or mitigate the effects of temporary or exceptional network congestion should not give providers of internet access services the possibility to circumvent the general prohibition on blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between specific content, applications or services, or specific categories thereof. Recurrent and more long-lasting network congestion which is neither exceptional nor temporary should not benefit from that exception but should rather be tackled through expansion of network capacity.*

For their part, the 2020 BEREC Guidelines (which were not revised in this regard in the 2022 update) set forth the following criteria in paragraphs 88 to 93:

- Management measures implemented to tackle network congestion may be preventive or reactive. But in all cases, they must be adopted on an exceptional or temporary basis.

- Two key considerations for NRAs are:

    - The proportionality of the measures adopted. In accordance with this principle, throttling of traffic is considered preferable to blocking it.

    - That these measures must not be used to circumvent the application of the general principles of net neutrality.

- The measures established must not discriminate between applications. This means that both the types of application concerned and the extent to which each of them is affected must be analysed.

- Because these measures may only be adopted on an exceptional and temporary basis, they may not be applied recurrently as a substitute for more structural solutions.

Practices analysed

On the basis of these exceptions, the general terms of contract offered by operators generally provide for the possibility of restrictions being placed on traffic due to network integrity, security or congestion issues.

The analysis conducted in 2019 identified that the contractual clauses providing for this type of measure were too generic, both as regards the nature of the specific measures that might be adopted to tackle network congestion and the duration of their implementation. As a result of the requirements laid down by SETELECO, the clauses have been duly amended to stipulate that, as demanded by the TSM Regulation, all traffic management measures are established on a temporary basis only and that they consist in prioritizing or deprioritizing certain types of traffic in the event of congestion, as detailed below:

- Deprioritizing traffic other than voice or video traffic, irrespective of the provider
- Prioritizing Voice over IP over other types of traffic
- Deprioritizing peer-to-peer (P2P) traffic
- Deprioritizing continuous mass mailing of spam messages that are prejudicial to other users

No significant developments were identified in this section in 2024.

Application in other European countries

As regards practices in other European countries, the BEREC Reports include the following:[34]

- Poland (2022). An audit revealed a breach of the terms of the TSM Regulation resulting from the practice of prioritizing business over retail customer traffic.
- United Kingdom. The following practices were investigated by the NRA and voluntarily abandoned by operators:
    - Throttling categories of traffic, such as P2P and virtual private network (VPN) traffic

[34] See APPENDIX III

- Prioritizing video and social media traffic over other types of traffic during periods of temporary network congestion

SETELECO criteria regarding offers that prioritize traffic on the grounds of network congestion:

Traffic management measures aimed at preventing network congestion are considered to be in accordance with the TSM Regulation provided that they meet the following requirements:

- **They are applied to complete categories of traffic and do not discriminate between applications, services or content within them**
- **They are conceived as temporary and exceptional measures in the terms of Article 3 of the TSM Regulation**

2.5 Specialized services

Regulation

Article 3(5) of the TSM Regulation refers to the provision of specialized services:

> *Providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services shall be free to offer services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality.*
>
> *Providers of electronic communications to the public, including providers of internet access services, may offer or facilitate such services only if the network capacity is sufficient to provide them in addition to any internet access services provided. Such services shall not be usable or offered as a replacement for internet access services, and*

shall not be to the detriment of the availability or general quality of internet access services for end-users.

Pursuant to Article 3(5), the lawful provision of specialized services is subject to the following requirements:

- The network must have sufficient capacity to provide them in addition to any internet access services provided.
- The services may not be offered as a replacement for internet access services.
- They must have no negative impact on the quality or availability of internet access services.

Paragraphs 99 to 127 of the 2022 BEREC Guidelines explore this matter at greater length, specifying, in essence, the following:

a) <u>Guidelines for NRAs</u>

- It must be determined whether the quality requirements are objectively necessary to ensure one or more key features of the service.
- Information may be demanded from the providers of these services on the relevant levels of quality (for example, as regards latency, jitter or packet loss). In addition, it should be demonstrable that these specific levels of quality cannot be assured over the IAS.
- It must be demonstrated that the level of quality cannot be assured by simply granting general priority over comparable content.
- It must also be determined whether optimization is objectively necessary. To this end, NRAs must assess whether the required level of quality cannot be assured by the internet access service itself.

b) <u>Requirements for specialized services</u>

- In relation to network capacity, services may not be provided if they cause a general degradation in the quality of general internet access.

- As for the prohibition on degrading access, quality measurements must be taken both when the service is being provided and when it is not.
- On mobile networks, no degradation is deemed to exist when the possible negative impact of the service is inevitable, minimal and limited to a short period of time. However, these unforeseeable impacts (related to the number of users and volumes) on traffic should not normally arise in fixed networks.
- As regards the requirement that these services not be used to replace internet access, the key issue is whether internet access provided by the specialized service is restricted, offers higher quality, or uses differentiated traffic management. If this were the case, the net neutrality regulation would not be deemed applicable to the service.

The 2020 BEREC Guidelines include the following addition:

a) Reliability of specialized services (paragraph 108). In principle, these services are justified objectively for technical QoS reasons. This, according to market operators, includes reliability. Nevertheless, they claim that device characteristics may be impeding reliability, especially in the case of resource-constrained devices, which can be affected by lack of power supply, interferences or security threats. These devices are characterized by their limited processing and storage capacity, and are usually battery powered.

   Operators have stated that, especially in the case of 5G, services such as M2M or Internet of Things (IoT) could include devices of this kind, which require specific network conditions. Operators believe this should be taken into consideration in the BEREC Guidelines.

   Accordingly, paragraph 108a of the BEREC Guidelines makes clear that requirements for a specific level of quality may not only refer to standard parameters, but may also apply to such parameters as processing power, for example, in novel networking paradigms such as IoT or M2M services.

b) Dedicated connectivity and logical separation of traffic. The 2020 BEREC Guidelines introduced two new paragraphs (110a and 110b) offering certain clarifications referring to dedicated connectivity between servers at the application layer and the logical separation of traffic between IAS and specialized services. According to the 2019 BEREC Public

Consultation, the previous Guidelines had been misinterpreted and clarifications were therefore proposed.

c) Improving the quality of service, especially with 5G. Improved performance in terms of QoS will lead to a situation where specialized services may no longer be necessary. In time, NRAs will have to reassess whether the requirements to provide these services are met.

The 2018 BEREC Opinion[35] delved deeper into this topic. It highlighted that BEREC Guidelines consider these services to be those that "do not provide general connectivity to the internet" and are "logically separated from the traffic of the IAS". As regards the first requirement, at network level, these services cannot be used to replace IAS with a service that prioritizes a specific application while providing internet access. At application level, there could be voice communication between a specialized service (Voice over Long-Term Evolution, or VoLTE) and an application (Skype). The user would not be connected to the internet and, therefore, it would not be understood to replace internet access and would be in line with regulations.

As regards the second requirement (logical separation), the BEREC Guidelines describe it as a possible method for the provision of this service rather than as a mandatory requirement. Therefore, it is not needed to provide the service.

Moreover, in relation to quality measurements that help determine the compatibility of the service with regulations, BEREC refers to a future measurement tool which it is designing.

Specialized services and 5G

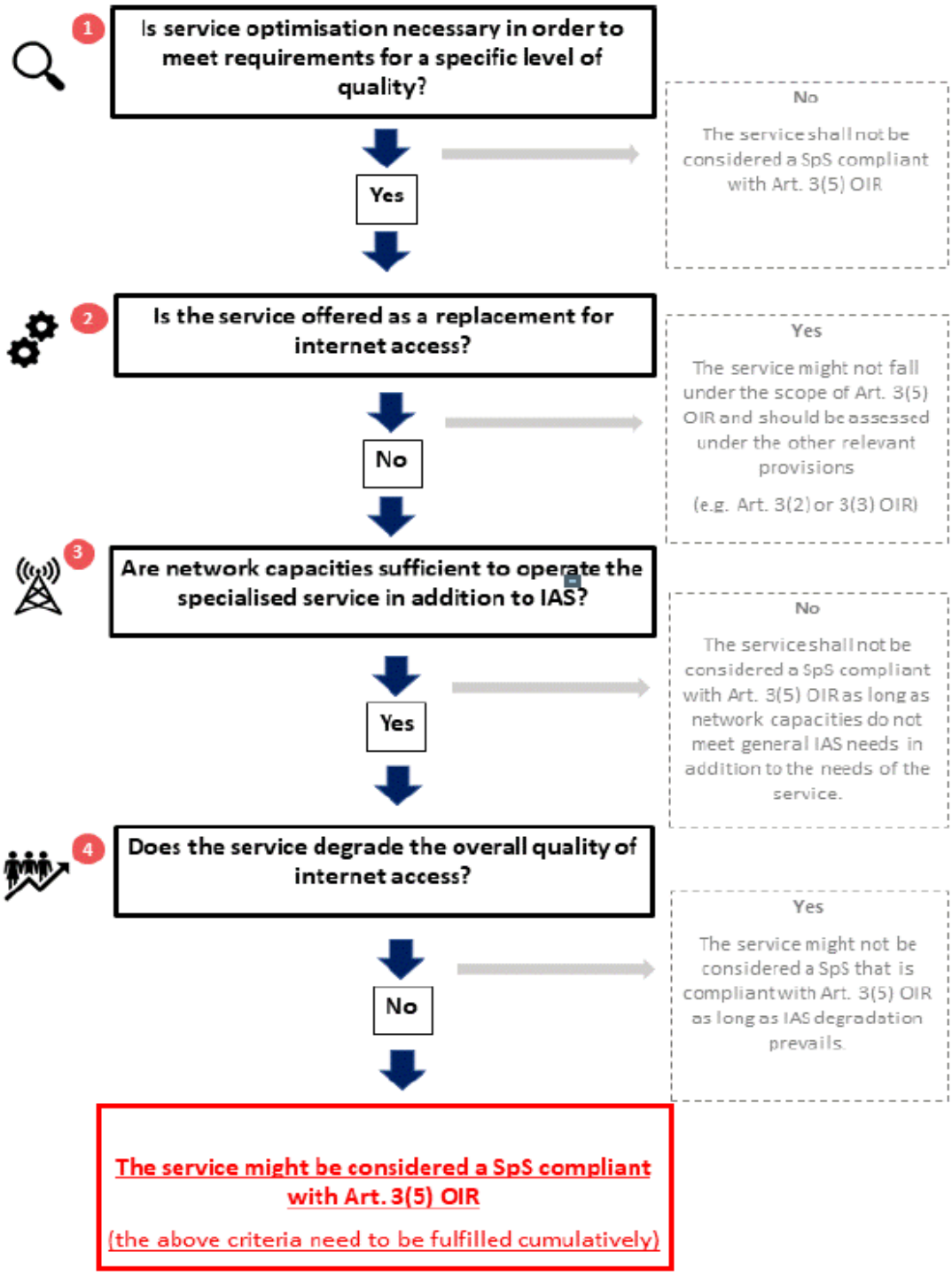
As stated in the section on traffic management measures, the arrival of 5G technology opens the door to the proliferation of specialized services. The techniques made possible by this technology (such as network slicing) make it ideal for providing services other than internet access, which entail specific requirements and do not harm overall quality.

[35]See APPENDIX III

The 2023 Commission Report points out the following in relation to specialized services:

> *The BEREC guidelines clarify how the rules in the Regulation should be understood by elaborating on the conditions for providing specialised services, which are provided in the Regulation itself. In this respect, the 2020 guidelines indicate that different applications (in the form of specialised services) can be treated differently when it is objectively necessary to meet an application's requirement for a specific level of quality that cannot be met over a best-effort internet access service. The BEREC guidelines acknowledge that the internet and the nature of internet access services will evolve over time. The three examples of specialised services, indicated in the BEREC guidelines and available in many Member States, are: VoLTE, IPTV, and VoIP.*
>
> *The assessment of compliance remains first and foremost with the provider considering to offer a specialised service, as no prior permission from NRA is required to offer such services to end-users. To establish whether a service is in- or out-of-scope, the Regulation requires internet access service providers to: (i) prove the need for each application to be treated in a particular way; (ii) show that it is separated from the internet access service; and (iii) demonstrate that such treatment will not have a negative impact for the end-users.*
>
> *[…]*
>
> *Greater legal certainty could therefore be beneficial to both innovators and consumers in the future. How to achieve it, by signalling that new high-performance services should be possible within the scope of the Regulation, and whether such 'signposting' should be done via a clarification in the BEREC guidelines (e.g. in shorter intervals commensurate with market and technological developments) or by the Commission, is one of the matters to focus on in the near future.*

In this regard, the aforementioned *Draft Further Guidance on 5G Network Slicing: Annex to the BEREC Guidelines on the implementation of the Open Internet Regulation* reiterates the criteria for self-assessment by operators of potential specialized services, and includes the following diagram:


1
Is service optimisation necessary in order to meet requirements for a specific level of quality?
Yes
No
The service shall not be considered a SpS compliant with Art. 3(5) OIR
2
Is the service offered as a replacement for internet access?
No
Yes
The service might not fall under the scope of Art. 3(5) OIR and should be assessed under the other relevant provisions
(e.g. Art. 3(2) or 3(3) OIR)
3
Are network capacities sufficient to operate the specialised service in addition to IAS?
Yes
No
The service shall not be considered a SpS compliant with Art. 3(5) OIR as long as network capacities do not meet general IAS needs in addition to the needs of the service.
4
Does the service degrade the overall quality of internet access?
No
Yes
The service might not be considered a SpS that is compliant with Art. 3(5) OIR as long as IAS degradation prevails.
The service might be considered a SpS compliant with Art. 3(5) OIR
(the above criteria need to be fulfilled cumulatively)

Offers analysed

As in previous years, the only clearly specialized service currently provided is Internet Protocol Television (IPTV). It is unclear whether this service can be net neutral in those cases in which the overall quality of internet access is affected, especially in networks which have a smaller capacity (DSL), the use of which is decreasing.

3. TRANSPARENCY MEASURES TO GUARANTEE OPEN INTERNET ACCESS

Article 4

Transparency measures for ensuring open internet access

1. Providers of internet access services shall ensure that any contract which includes internet access services specifies at least the following:
    a. information on how traffic management measures applied by that provider could impact on the quality of the internet access services, on the privacy of end-users and on the protection of their personal data;
    b. a clear and comprehensible explanation as to how any volume limitation, speed and other quality of service parameters may in practice have an impact on internet access services, and in particular on the use of content, applications and services;
    c. a clear and comprehensible explanation of how any services referred to in Article 3(5) to which the end-user subscribes might in practice have an impact on the internet access services provided to that end-user;
    d. a clear and comprehensible explanation of the minimum, normally available, maximum and advertised download and upload speed of the internet access services in the case of fixed networks, or of the estimated maximum and advertised download and upload speed of the internet access services in the case of mobile networks, and how significant deviations from the respective advertised download and upload speeds could impact the exercise of the end-users' rights laid down in Article 3(1);
    e. a clear and comprehensible explanation of the remedies available to the consumer in accordance with national law in the event of any continuous or regularly recurring discrepancy between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated in accordance with points (a) to (d).

    Providers of internet access services shall publish the information referred to in the first subparagraph.
2. Providers of internet access services shall put in place transparent, simple and efficient procedures to address complaints of end-users relating to the rights and obligations laid down in Article 3 and paragraph 1 of this Article.

3. The requirements laid down in paragraphs 1 and 2 are in addition to those provided for in Directive 2002/22/EC and shall not prevent Member States from maintaining or introducing additional monitoring, information and transparency requirements, including those concerning the content, form and manner of the information to be published. Those requirements shall comply with this Regulation and the relevant provisions of Directives 2002/21/EC and 2002/22/EC.
4. Any significant discrepancy, continuous or regularly recurring, between the actual performance of the internet access service regarding speed or other QoS parameters and the performance indicated by the provider of internet access services in accordance with points (a) to (d) of paragraph 1 shall, where the relevant facts are established by a monitoring mechanism certified by the national regulatory authority, be deemed to constitute non-conformity of performance for the purposes of triggering the remedies available to the consumer in accordance with national law.
   This paragraph shall apply only to contracts concluded or renewed from 29 November 2015.

3.1 Current legislation

In general terms, the rights of users of electronic communications services are specifically protected by the GTA, and the Electronic Communications Services Users Charter (Royal Decree 899/2009, of 22 May).

In Spain, current regulations require that, in addition to the users concerned, SETELECO be notified of all contracts and of any amendments thereto.

SETELECO analyses the content of contracts and any amendments thereto to determine whether they are in line with Spanish and EU regulations on the protection of end-users of electronic communications services.

Any amendment of contract conditions by operators must be notified to all the customers concerned one month in advance. The operator must notify the end-user of their right to terminate the contract at no extra cost, unless the proposed changes exclusively benefit the end user, or are strictly administrative in nature and have no negative impact on end users, or are required by regulations.

3.2 Traffic management measures in contracts

Since the GTA was passed, operators have adapted their contracts to include:

- Possible limits on the use of services
- Possible restrictions on the use of the device provided

- Information on any condition limiting access or use of services and applications
- Information on any procedures established by the operator to measure and shape traffic in a way that avoids filling or overfilling the network link, and information on the manner in which said procedures might affect QoS
- The kinds of measures that the operator may take in case of security or integrity incidents, threats or vulnerability

In general, the net neutrality clauses contained in contracts notified by operators are increasingly specific. The cases in which these measures can be applied are listed and a time frame given in which they will be carried out, unless they are permanent.

Operators include clauses that are aligned with the management measures permitted under the TSM Regulation. These include:

a) Reasonable traffic management measures (Article 3(3) of the TSM Regulation)

- Non-discriminatory compression techniques, which reduce the size of data files without modifying their content
- In fixed wireless accesses, limits on the available bandwidth for quality reasons, given that it is a shared resource

b) Traffic management measures for reasons of network integrity and security (Article 3(3)b of the TSM Regulation)

- Websites blocked only on court orders
- Restriction of traffic when DDoS attack detected; in such cases, traffic is redirected to units that block illicit data trafficking
- Blocking of port 25 to avoid spam or malware

c) Traffic management measures to avoid network congestion or saturation (Article 3(3)c of the TSM Regulation)

- Only in case of congestion: discard traffic which is neither voice nor video, regardless of provider
- Prioritization of Voice over Internet Protocol (VoIP) over other kinds of traffic
- Deprioritization of P2P traffic
- In general, possibility of slowing traffic during periods of temporary congestion

3.3 Limits on data volumes

In general, operator contracts include clear explanations of limits on data volumes, as well as explanations of the consequences of reaching said limits in terms of user experience and prices. Observed changes are as follows:

- There are usually no limits on data volumes in flat-rate offers linked to landlines.
- In the case of mobile services, reaching the limit leads to a drastic reduction in access speed, thus avoiding bill shock.
- Operators offer additional data bundles once the limit has been reached, in order to enable customers to continue using the internet at the highest speed available.

Data roaming limits are a different issue. Operators frequently state the limits provided for in Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast) and in Commission Implementing Regulation EU 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment. The resulting limit equals the price of the bundle divided by the regulated wholesale data roaming price (€1.30/GB in 2025, excluding VAT) and multiplied by two.

SETELECO examines every offer to ensure that possible data roaming limits are in line with the aforementioned EU Regulations.

Unlimited data offers

The first unlimited data offers for mobile networks–offering unlimited data usage–became available in 2019. The availability of these offers could have positive impacts on some aspects related to net neutrality. This has been the case with zero rating offers: as the availability of unlimited data offers has increased, the importance of zero rating offers has decreased, regardless of court cases on their validity.

However, other aspects of the surge in unlimited data offers should be analysed from a net neutrality perspective, as operators could consider imposing "fair use" clauses to avoid the disproportionate or abusive use of the offer. This happened in previous years with voice services: operators introduced clauses limiting the number of lines which could be called and banning the use of devices such as SIMBOX, which allowed users to re-sell the service.

Actions taken in 2025

Clauses relating to data service–which affects net neutrality–were analysed to ensure compliance with regulations. Specifically, the following clause types were analysed:

a) Restrictions on the use of multi-SIM cards on devices other than mobile phones:

   - The reach of restrictions placed on mobile data offers by operators is being monitored.

b) Restrictions on data roaming inside and outside the European Union. The correct application of the formula for roaming data availability has been monitored.

3.4 Internet access speeds in contracts

Applicable regulation

As regards those access speeds that must be stipulated in contracts, in previous years the main operators were requested to bring their contracts into line with Article 4(1)d of the TSM Regulation, which states:

> *d) a clear and comprehensible explanation of the minimum, normally available, maximum and advertised download and upload speed of the internet access services in the case of fixed networks, or of the estimated maximum and advertised*

download and upload speed of the internet access services in the case of mobile networks, and how significant deviations from the respective advertised download and upload speeds could impact the exercise of the end-users' rights laid down in Article 3(1);

This means the following kinds of access speed must be stipulated:

- Fixed networks: maximum speed, advertised speed, minimum speed and normally available speed, both for uploads and downloads

- Mobile networks: maximum speed and advertised speed, both for downloads and uploads

The 2022 BEREC Guidelines provide direction on interpreting the different kinds of speed which should be stipulated in contracts. There have been no changes in this regard in the most recent Guidelines. Of particular interest is the guidance regarding fixed network speeds:

- Minimum speed (paragraphs 143-144):
  - This is considered to be the actual speed achievable at any given moment.
  - NRAs may set requirements for the minimum speed defined in contracts, such as a proportion between minimum and maximum speed.

- Maximum speed (paragraphs 145-146):
  - The maximum speed is the speed that an end-user could expect to receive at least some of the time (e.g. once a day).
  - NRAs may set requirements, such as the number of times the speed is achievable over a period of time.

- Normally available speed (paragraphs 147-149):
  - The normally available speed is the speed that an end-user could expect to receive most of the time. BEREC considers that the normally available speed has two dimensions: the numerical value of the speed and the availability (as a percentage) of the speed during a specified period.

- NRAs may use their own criteria to establish a percentage of peak and off-peak hours; or set an obligatory proportion with respect to maximum speed.

The only significant addition included in the 2019 BEREC Public consultation[36] in this regard refers to the speed which must be stipulated in contracts for fixed access using wireless technology, discussed below.

Fixed access networks via wireless technology

These networks set a particular challenge regarding the speeds to be stipulated in contracts. They provide end-users with fixed internet access, and should therefore be subject to the provisions on speed set forth in Article 4(1)d, which requires contracts to contain "a clear and comprehensible explanation of the minimum, normally available, maximum and advertised download and upload speed of the internet access services".

However, it must be borne in mind that these networks use wireless technologies to provide access, thus constituting shared resources. This would make them similar to mobile networks, meaning it would only be necessary for maximum and advertised speeds to be specified in contracts. Contracts for this kind of access analysed in Spain tend to include maximum and advertised speeds only.

The 2020 BEREC Guidelines offer specific guidance in this regard, incorporating changes seeking to clarify how "hybrid internet access services" and certain "fixed wireless accesses" (FWA) should be treated for transparency purposes.

BEREC recognizes that a certain level of uncertainty may exist regarding transparency rules applied to mobile or fixed networks. The changes to the Guidelines aim to clarify under which conditions BEREC considers a network to be included in either category.

Two new paragraphs were added (141a and 141b):

- The first paragraph equates certain types of FWA with fixed network services, referring specifically to the use of wireless technology networks (including mobile networks) to

[36] See APPENDIX III

provide internet access at a fixed location with dedicated equipment, applying either capacity reservation or the usage of a specified frequency spectrum band. In such cases, the transparency requirements for fixed networks are applicable.

- The second paragraph asserts that BEREC considers hybrid access as fixed network access when it consists of a combination of fixed and mobile technologies as a single subscription, it is provided at a fixed location and is marketed as a fixed service. In this case, transparency requirements for fixed networks are applicable.

  Nevertheless, unless all of the aforementioned conditions are met, fixed network requirements will be applicable to the fixed part of the contract and mobile network requirements will be applicable to the mobile part of the network.

Reflection on the different kinds of speed in operator contracts

Until 2016, operators usually only included in their contracts a reference to the information on internet access speed that was published on their websites. However, this failed to meet the requirements of Article 4(1)d of the TSM Regulation, which requires any contract including an internet access service to contain "a clear and comprehensible explanation of the minimum, normally available, maximum and advertised download and upload speed of the internet access services".

Therefore, the information must appear in a document constituting part of the contract. This may be the general conditions, the specific conditions, or the contract summary document where customer data and contracted services appear.

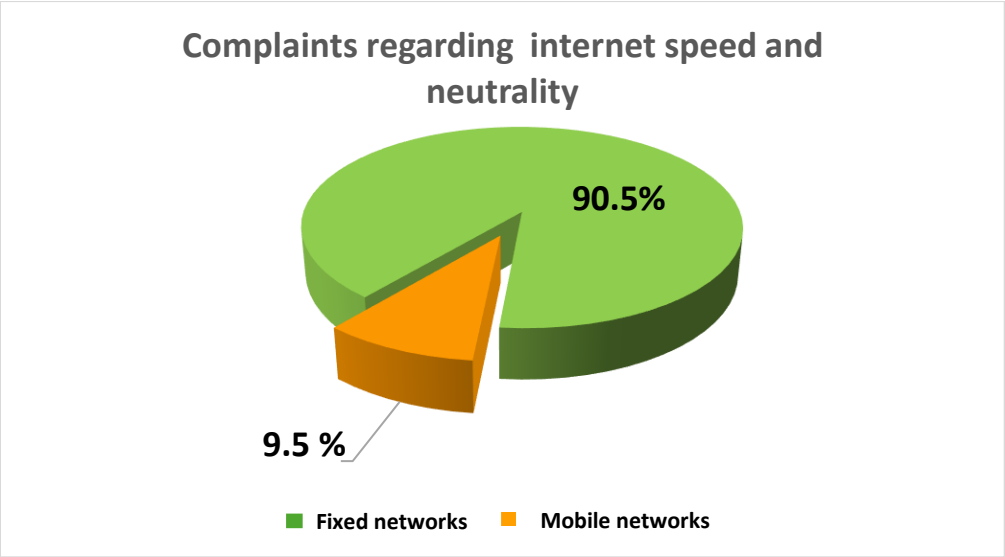
Operators have therefore adapted their contracts to these requirements. Most operators have chosen to include a summary in the form of a table of the different technologies and modalities (e.g. Digital Subscriber Line (DSL), FTTH) they sell. Operators are required to include the speed of each modality for each offer they place on the market. The remaining operators have chosen to include speeds in the specific conditions, or in the rate table given to the end-user with their contract when subscribing to a service.

3.5 Disputes regarding internet access speeds

Article 4(4) of the TSM Regulation states as follows.

Any significant discrepancy, continuous or regularly recurring, between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated by the provider of internet access services in accordance with points (a) to (d) of paragraph 1 shall, where the relevant facts are established by a monitoring mechanism certified by the national regulatory authority, be deemed to constitute non-conformity of performance for the purposes of triggering the remedies available to the consumer in accordance with national law.

It must be borne in mind that the TUAO of the Ministry of Digital Transformation and the Civil Service receives very few complaints concerning internet speed. In 2025, only 0.32% of complaints received by the Office related to internet speed. The vast majority (90.5%) of said complaints referred to fixed networks, while only 9.5% referred to mobile networks.



Complaints received by the TUAO regarding internet access speed in 2025

Article 4(4) makes clear that failing to deliver internet access at the different kinds of speed provided for in the TSM Regulation and reflected in the operator's conditions shall constitute an individual breach of contract by the company. The determining criteria are for a "significant discrepancy" to exist between the actual speed and that specified in the contract and for said discrepancy to be "continuous or regularly recurring". This means measurements need to be taken over a period of time.

Therefore, multiple aspects must be considered in connection with this issue, and since 2018, the administration has been analysing it closely in collaboration with operators.

a) Monitoring mechanism

In Spain, a certified "monitoring mechanism", to use the term employed in the Regulation, capable of assessing compliance with legislation, has not yet been adopted. This issue is considered especially complex due to the environment and conditions in which measurements of speed would have to be taken for them to constitute reliable results. Measurements must be taken by connecting directly to the router. This avoids interference due to the use of wireless technology (measurements taken after the Wi-Fi router) as well as possible problems with the cable installed inside the end-user's home.

Moreover, the mechanism must rule out any influence from other undesirable factors such as other devices being connected to the router at the time the measurement is taken or the device used to run the measurement programme having insufficient power.

It should be borne in mind that BEREC has been working to create a tool to enable the measurement of quality parameters, such as speed. The 2018 BEREC Opinion[37] considers this an essential element for NRAs to make determinations on this and other aspects. Another essential element is whether specialized services are having an impact on the general quality of internet access services. This aspect is also mentioned in the 2019 Commission Report.[38]

SETELECO, in collaboration with operators, has explored mechanisms to resolve users' complaints, which have proven satisfactory.

In this regard, it should be highlighted that when operators receive complaints from users regarding internet speed it is rare for them to question the user's experience. Usually, when the internet speed experienced by the user is below what was provided for in the contract, the operator recognizes the problem and seeks to solve it by adapting the tariff to the speed the customer enjoys. If this is not possible, operators will allow users to terminate the contract without incurring any kind of penalty.

[37] See APPENDIX III

[38] See APPENDIX III

To date, SETELECO's preferred method for taking measurements has been remote measuring by operators. This option allows the influence of factors which could impact measurements if a user were acting in an unreliable environment (wireless connection to the router or use of a deficient device) to be ruled out.

In this regard, the GTA includes the following provisions:

Article 69. Quality of service.

1. The National Markets and Competition Commission, following a report issued by the State Secretariat for Telecommunications and Digital Infrastructure, shall specify the quality of service parameters to be measured, the applicable measurement methods, and the content, form and manner of the information to be published, including possible quality certification mechanisms. To this end, BEREC guidelines shall be taken into account and the parameters, definitions and measurement methods set out in Annex X of the European Electronic Communications Code shall be used.

2. The National Markets and Competition Commission may require operators of internet access services and of publicly available interpersonal communications services to publish comprehensive, comparable, reliable, user-friendly and up-to-date information for end-users on the quality of their services, to the extent that they control at least some elements of the network either directly or by virtue of a service level agreement to that effect, and on measures taken to ensure equivalence in access for end-users with disabilities.

The National Markets and Competition Commission may also require operators of publicly available interpersonal communications services to inform consumers if the quality of the services they provide depends on any external factors, such as control of signal transmission or network connectivity.

If the National Markets and Competition Commission requests said information, it must be supplied prior to publication.

The National Markets and Competition Commission shall conduct a study on the quality of service offered to end-users living in rural and sparsely populated areas in comparison with the average quality of service offered to users living in the rest of the country.

The measurements established by operators of internet access services and of publicly available interpersonal communications services to guarantee the quality of their services shall be in line with Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic

communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

b) Types of fixed network

Discrepancies between contractual and actual speeds necessitating measurements also appear in DSL access networks. Complaints regarding speed in FTTH networks, although possible, do not require measurements, as this kind of access guarantees the speed received by the end-user. In fact, complaints received show a solution is usually found immediately, as the problems are caused by a breakdown or simply by mistakes in the line provision procedure, leading to adapted speeds being offered to the user.

c) Speed reflected in contracts

Analysis of speed tables published by operators in contracts and on websites reveals the following:

- In the case of FTTH networks, average ("normally available") speed is generally the same as maximum speed. Nevertheless, some operators state that it is around 85% of maximum speed. Minimum speed is given as between 50% and 92% of maximum speed, depending on the operator.

- In the case of fixed DSL networks, minimum speed is usually between 30% and 40% (although some operators give minimums of 5%), while normally available speed is between 50% and 60% of maximum speed.

- For 4G mobile networks (some operators publish speeds for their 4G+ variant), speed ranges between 300 Mbps and 40 Mbps (download), and 20 Mbps and 150 Mbps (upload).

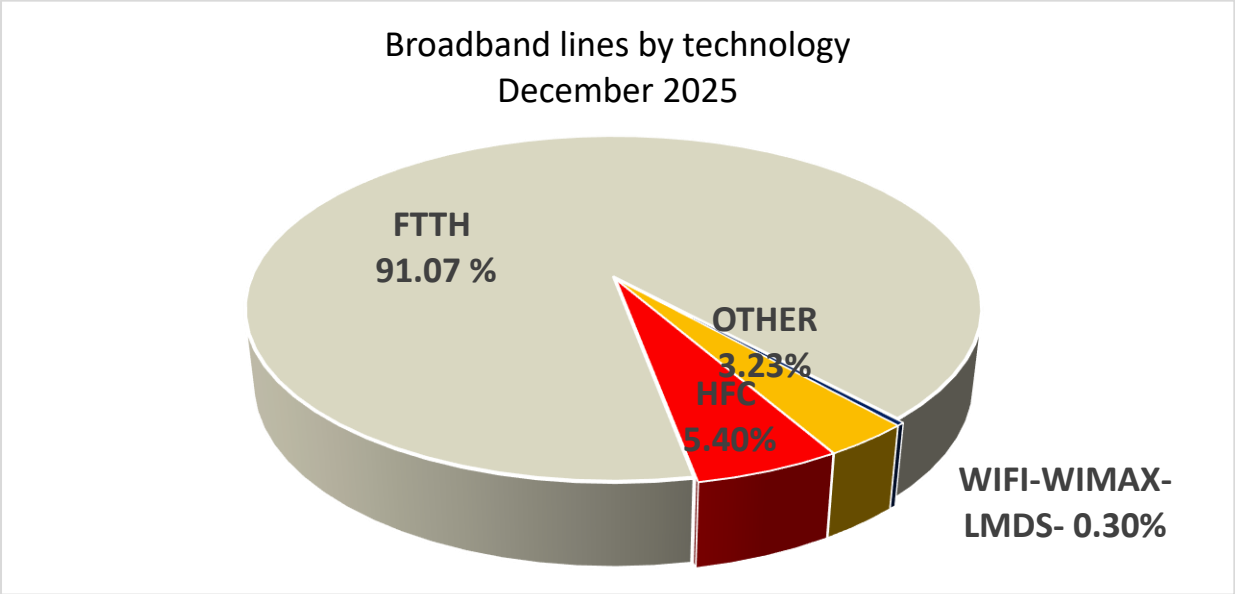
- For 5G mobile networks, speed ranges between 1,000 Mbps and 1,600 Mbps (download), and 45 Mbps and 200 Mbps (upload).

In the establishment of facts called for by Article 4(4) of the TSM Regulation, it will be these speeds that will be taken into account when examining individual complaints over insufficient internet speed.

According to data from the CNMC, FTTH accesses are currently far more common than DSL accesses. Although DSL is more liable to generate complaints, its decline in use should lead to a drop in complaints.

Data for 2025 published by the CNMC is as follows:

Dec-25	FIXED BROADBAND LINES BY TECHNOLOGY	
	(thou.)	%
FTTH	17,793	91.07%
HFC	1,055	5.40%
OTHER	631	3.23%
WIFI-WIMAX-LMDS	58	0.30%
TOTAL	19,537	



Source: *CNMC: Retail fixed broadband lines by technology. December 2025*

d) Consequences of discrepancies

A decision must be made regarding the rights to be recognized to users whose complaints are upheld because actual speed is found not to match contractual speed. Analysis conducted in 2025 concludes that three different kinds of rights can be recognized:

- Economic compensation due to breach of contract
- The right to terminate the contract without incurring any kind of penalty for breach of contract
- The obligation for the operator to adapt contract conditions to the actual speed

e) Conclusions

Although over the course of 2025 progress was made in the analysis of the aforementioned aspects, the complaint and measurement system regarding internet access speed is expected to be rolled out gradually. To date, the most significant problems detected are as follows:

- The speeds that operators include in DSL contracts, taking into account that several individual factors have an impact on the speed of each line

- Establishment of a speed measurement system whereby the reliability of the results obtained is proportionate to the resources allocated

3.6 Complaints regarding internet access speeds

- **As regards the remedies made available to users** in cases of non-compliance with Article 4(4) of the TSM Regulation, the main procedure entails lodging a complaint with the TUAO at the Ministry of Digital Transformation and the Civil Service.39

[39] www.usuariosteleco.gob.es

Since 2005, the TUAO has processed and adjudicated complaints made by citizens against operators in the exercise of their rights as end-users of electronic communications services.

This is an out-of-court settlement procedure for operators and end-users. Its main characteristics are as follows:

- All operators must submit to this procedure.
- The procedure concludes with a decision that is binding for both parties. The operator is therefore required to comply with the Office's decision.
- It is a quick and flexible procedure: In December 2018, the average processing time was 4.3 months (below the legal maximum of 6 months).
- The procedure is free for users.

In 2025, TUAO received a total of 12,454 complaints.The TUAO is competent to adjudicate complaints concerning breaches of the TSM Regulation. Nevertheless, in 2025 only 2.45% of complaints referred to network neutrality, and of these, 0.32% referred to slow internet access. As a consequence of processing said complaints, it was observed that operators generally fulfil their contractual obligations.

To conclude, in general terms, this matter is not a significant issue for end-users in Spain.

- **Publication of information.** It should be noted that operators are obliged to publish the general conditions of all the different types of contract they offer to customers on their websites. Therefore, insofar as the content analysed in the previous sections is required to appear in contracts, it must also be published, subject to the transparency requirements established by the GTA and the Electronic Communications Services Users Charter.

- **Complaints to the operator.** According to Spanish regulations to protect electronic communications service users, operators are required to have customer services departments that process enquiries and complaints and, more broadly, that handle all incidents relating to contracts. In this regard, the Electronic Communications Services Users Charter establishes the following obligations:

  - The service must be free for the customer.

- Users must always be offered the possibility of obtaining written proof of procedures conducted over the telephone.
- Users must always be offered the option of lodging complaints over the telephone, and provided with a reference number by which to follow up their complaint.
- Complaints must be processed within a one-month period. Otherwise, it will be understood that the requirement for the user to lodge a complaint with the operator before lodging a complaint with the TUAO has been met.

All the rights included in the TSM Regulation are considered rights of users of electronic communications services and may therefore form the basis of complaints lodged with operators, as described above.

4. SUPERVISION AND ENFORCEMENT

Article 5. Supervision and enforcement.

1. National regulatory authorities shall closely monitor and ensure compliance with Articles 3 and 4, and shall promote the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology. For those purposes, national regulatory authorities may impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate and necessary measures on one or more providers of electronic communications to the public, including providers of internet access services.

National regulatory authorities shall publish reports on an annual basis regarding their monitoring and findings, and provide those reports to the Commission and to BEREC.

2. At the request of the national regulatory authority, providers of electronic communications to the public, including providers of internet access services, shall make available to that national regulatory authority information relevant to the obligations set out in Articles 3 and 4, in particular information concerning the management of their network capacity and traffic, as well as justifications for any traffic management measures applied. Those providers shall provide the requested information in accordance with the time-limits and the level of detail required by the national regulatory authority.

4.1 System designed

Article 69 of the GTA accords powers to the CNMC to establish the QoS parameters and the applicable measurement methods, as well as the content and format of the information to be made public, including possible quality certification mechanisms.

The CNMC used these powers in the Decision issued on 23 January 2025, which established QoS parameters for electronic communications and methods for measuring them[40].

Said Decision states that, on 21 September 2022, the CNMC conducted a public consultation in which it asked the sector, among other matters, about the model for measuring quality parameters and about possible improvements. The following answers were given:

- Publication of quality measurement results through a user-friendly interface.
- Rationalization of parameters to be published, deleting those which are the least relevant for end-users owing to changes in markets and technological developments. Addition of new parameters that may be of interest to end-users in line with the BEREC Guidelines and the IAS parameters (latency, jitter and packet loss) that appear in Annex X of the European Electronic Communications Code.
- Mid-term review of the current measurement system with the aim of reducing costs for operators, making it more representative in geographical terms, and improving users' access to data.

Specifically, the quality of service of the internet access system has become the most important feature for end-users, as it is this aspect that has seen the greatest changes, from speeds of hundreds of kilobits per second to speeds of megabits per second and even gigabits per second, and it is also key for all over-the-top services such as video streaming, gaming, etc. Therefore, the quality of service of the internet access system has a direct impact on the performance of these services.

It is therefore clear that QoS parameters for internet access systems must continue to be measured and published. Moreover, these measurements must continue to be taken

[40] https://www.cnmc.es/sectores-que-regulamos/telecomunicaciones/calidad-servicios

separately for fixed connections and mobile networks, as these services have very different technical characteristics which directly impact on the quality of service offered to users.

The Decision bases its QoS parameters for internet access systems on the aforementioned Order IET/1090/2014 (data transmission speed for both uploads and downloads) and states the need to also measure the following parameters:

(i) packet loss
(ii) delay
(iii) jitter

These parameters are increasingly important to the end-user because the internet access system has become a service which not only makes it possible to browse websites but also enables the provision of many other services, including over-the-top services. As it communicates in real time, it is sensitive to both delay and jitter.

In addition, the inclusion of these three parameters in both Annex X of the European Electronic Communications Code and in the BEREC Guidelines is indicative of their significance in allowing the end-user to assess the quality of internet connections offered by different market providers, and whether it meets their needs.

As a result, it is understood that the following QoS parameters for internet access systems must be measured:

(i) internet access upload and download speed
(ii) delay
(iii) jitter
(iv) packet loss

Lastly, it must be highlighted that the Decision considers that, taking into account the services being measured and the measurement system to be implemented, the obligation to measure and publish QoS parameters must be met by those operators listed in the CNMC Operator Register with an annual turnover above 20 million euros, taking into account each of the services measured separately.

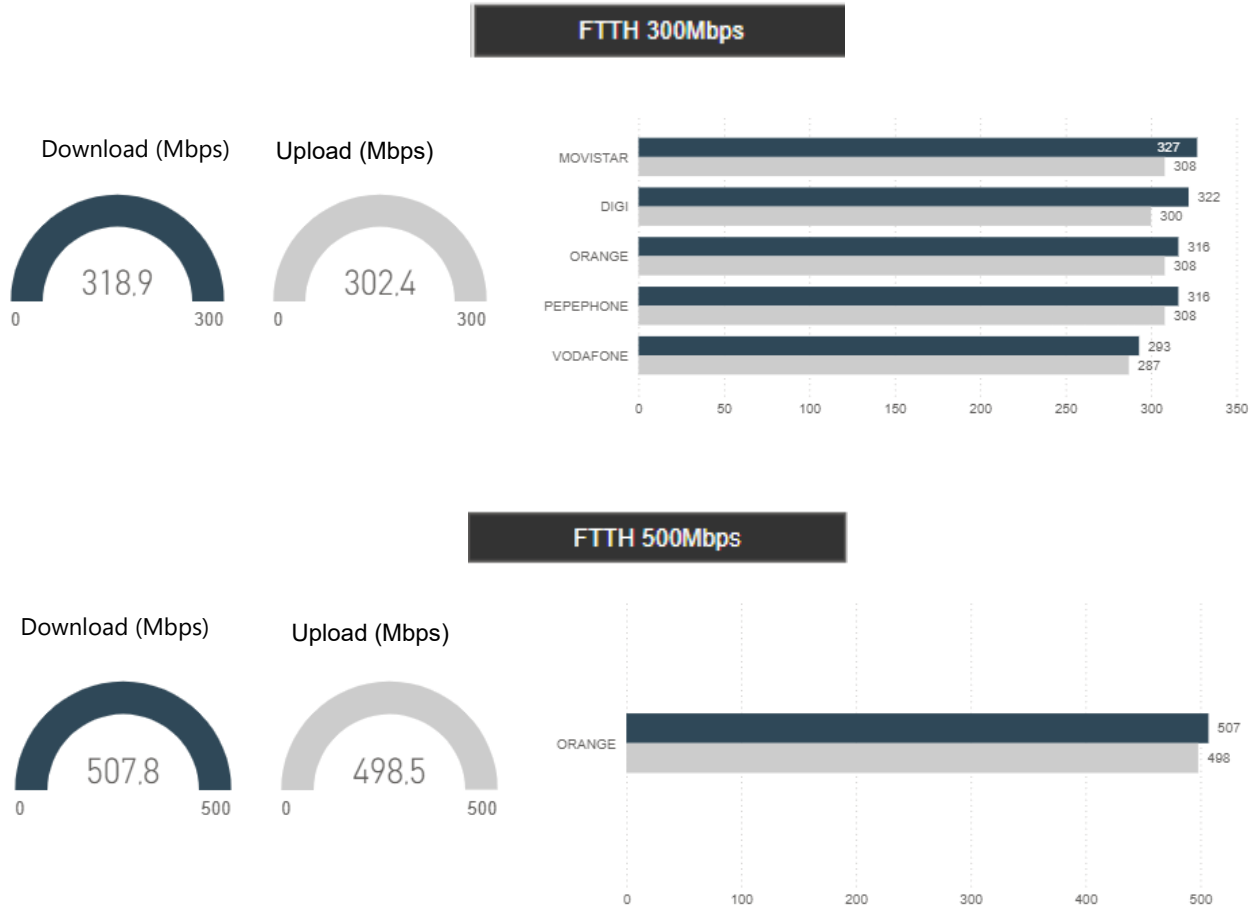
4.2 Results obtained

Every quarter the CNMC publishes the values obtained from the measurement of quality levels on a user-friendly interface. This facilitates comparisons between technologies, commercial offers (speeds) and operators.

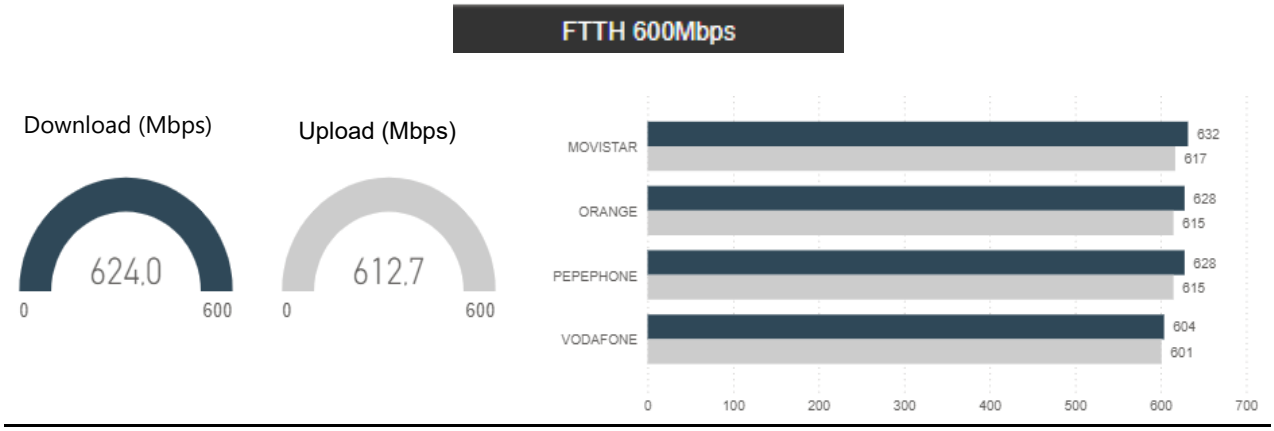
Below are some of the results published in the fourth quarter of 2025[41] (weighted average speeds and operator ranking by upload and download speeds).

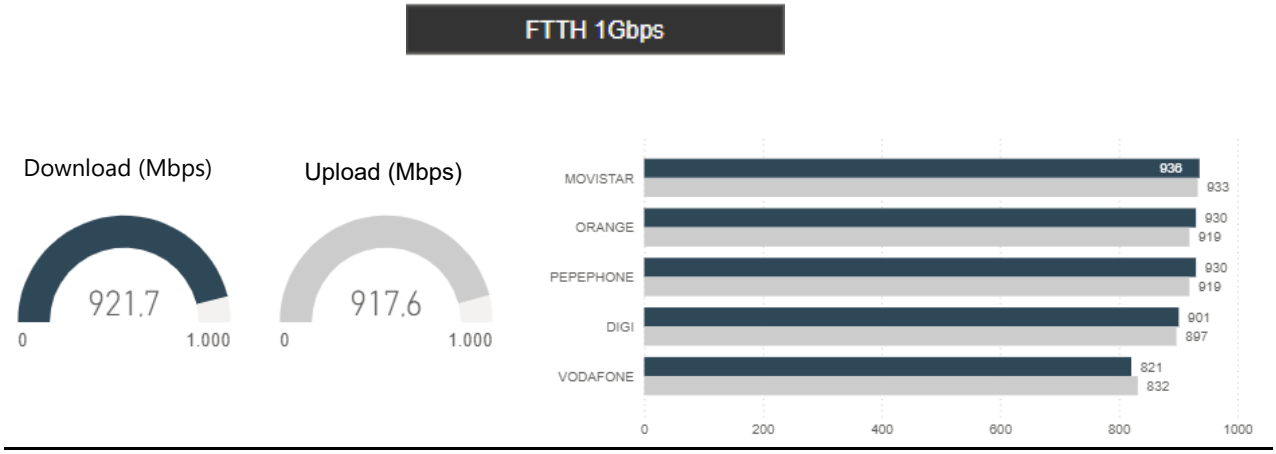
Summary of Internet Access Speed 2025 Q4

FIXED INTERNET ACCESS SERVICE

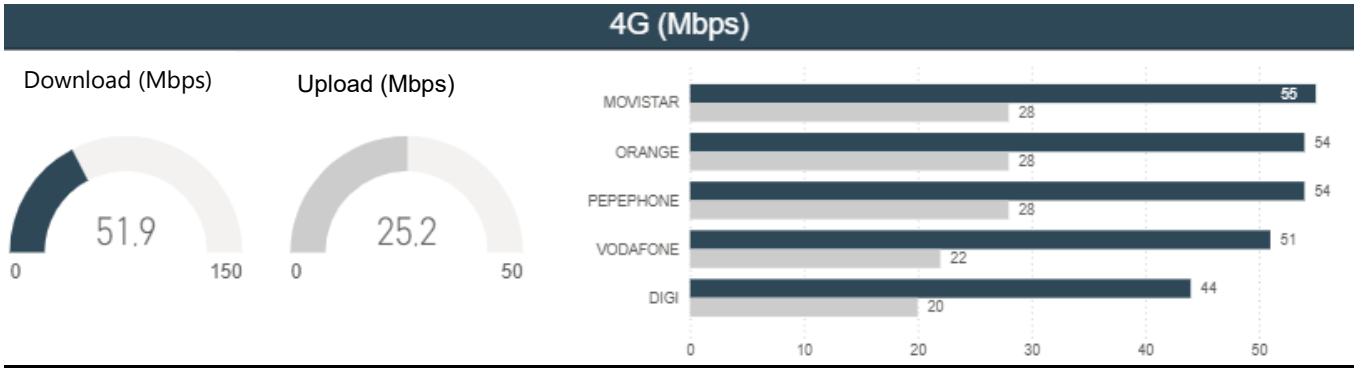


[41] https://avancedigital.mineco.gob.es/es-es/Servicios/CalidadServicio/informes/Paginas/Informes09.aspx





MOBILE INTERNET ACCESS SERVICE



LINKS OF INTEREST

In this section, we provide links by which to access the QoS results published by Spanish operators that have been used to prepare this report. Links to other European regulators which have published QoS results obtained in their fields are also provided.

SPAIN

OPERATOR	Link
DIGI	https://www.digimobil.es/legal-calidad.php
euskaltel	http://www.euskaltel.com/CanalOnline/microsites/calidad_servicio/index.jsp?idio
Jazztel	https://www.jazztel.com/accesible-calidad.html
MÁSMÓVIL	https://www.masmovil.es/static/pdf/calidad-servicio-mm.pdf
movistar	https://www.telefonica.es/es/acerca_de_telefonica/calidad/calidad-servicio
orange	https://www.orange.es/acercadeorange/calidad
pepephone	https://www.pepephone.com/calidad-del-servicio
R	https://mundo-r.com/quienes-somos/calidad-de-servicio
telecable	http://web.telecable.es/calidad-servicio
vodafone	https://www.vodafone.es/c/conocenos/es/vodafone-espana/calidad/calidad-de-servicio/
yoigo	https://www.yoigo.com/calidad-de-servicio

masorange	https://masorange.es/

EUROPEAN REGULATORS

REGULATOR	Link
TRAFICOM Finnish Transport and Communications Agency (FI)	https://www.traficom.fi/en/etusivu
arcep (FR)	https://en.arcep.fr/
EETT HELLENIC TELECOMMUNICATIONS & POST COMMISSION (GR)	https://www.eett.gr/en/
Commission for Communications Regulation (IR)	https://www.comreg.ie/
AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI AGCOM (IT)	https://www.agcom.it/
ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES (PT)	https://www.anacom.pt/

National Markets and Competition Commission

CNMC COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA	https://www.cnmc.es/en/ambitos-de-actuacion/telecomunicaciones

4.3 Information provided by operators

As regards powers to monitor compliance with Articles 3 and 4 of the TSM Regulation, it is important to highlight the following:

- Pursuant to the TSM Regulation and the GTA, SETELECO may request that operators submit all information and documents necessary to monitor their compliance with net neutrality obligations.

- In general terms, the GTA authorizes SETELECO to request that operators provide all the information it needs to monitor their compliance with telecommunications regulations.

  Article 76(9) of the GTA provides that:

  > *The Ministry of Economic Affairs and Digital Transformation* [whose powers are currently exercised by the Ministry of Digital Transformation and the Civil Service] *shall monitor the application of this Article and shall publish an annual report on said monitoring and its results, which it shall forward to the National Markets and Competition Commission, the European Commission and BEREC. To conduct said monitoring, the Ministry of Economic Affairs and Digital Transformation may request that operators of publicly available electronic communications, including operators of IAS, provide relevant information with the necessary degree of detail to verify compliance with the obligations set forth herein and, in particular, information on the capacity and traffic management of their network. In addition, the Ministry may request submission of documents evidencing all traffic management measures applied.*

In addition, failure to answer or to supply the information and documents required is classed by the GTA as a serious infringement (subject to a maximum penalty of 2 million euros).

5. PENALTIES

Article 6

Penalties

Member States shall lay down the rules on penalties applicable to infringements of Articles 3, 4 and 5 and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by 30 April 2016 and shall notify the Commission without delay of any subsequent amendment affecting them.

Articles 3, 4 and 5 of the TSM Regulation refer to:

- Article 3: Safeguarding of open internet access
- Article 4: Transparency measures for ensuring open internet access
- Article 5. Supervision and enforcement

As regards the net neutrality obligations established by the TSM Regulation, the GTA contains the necessary elements to penalize infractions.

Section Two of Final Provision Four ("Incorporation of European Union Law") of the GTA provides as follows:

This Act adopts the measures to enforce or apply the following Regulations:

[…]

b) Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

5.1 Sanctioning power

The offences and penalties established by the GTA give the Spanish State (and within it, the Ministry of Digital Transformation and the Civil Service) the powers to impose penalties for breaches of the provisions of the TSM Regulation. Specifically, it provides for the following offence:

- 107(40): breach of the obligations established in Article 76 and implementing regulations as well as Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015.

Therefore, any breach of the obligations established by the TSM Regulation and the GTA will be penalized in accordance with one of these provisions. In the case of serious infringements (Article 109.2), penalties may amount to up to 2 million euros.

In 2025, the supervisory authorities continued to focus on the adaptation of operator contracts to the provisions set forth in Article 4 of the TSM Regulation. A joint analysis was conducted of practices which could be in breach of (or admissible under) Article 3 of the Regulation to ensure that admissible practices may be reflected in contracts.

The aforementioned analysis did not identify any practices that were in breach of the TSM Regulation and therefore subject to a penalty. Possible discrepancies with the TSM Regulation, listed in this report, were solved informally: SETELECO's interpretations of the Regulation were accepted by operators, which changed or removed the offers concerned.

The 2023 Commission Report contains a reference to Member States' systems for penalizing infractions.

> *Sanctions and the methods for calculating penalties differ widely between Member States. For example, 13 Member States have set penalties linked to the company's turnover, while others have a fixed maximum amount or a combination of the two. The maximum penalties vary from 0.25% to 5% of the average annual worldwide turnover, or are set at a maximum amount which ranges from EUR 100 000 to EUR 5 million. Only a few penalties have been imposed to date, and all of them were well below the applicable maximum.*

5.2 Powers of inspection and supervision

Powers of inspection shall be complementary to sanctioning powers. The Ministry of Digital Transformation and the Civil Service has the necessary powers of inspection concerning electronic communications networks and services provided for in Articles 103 et seq. of the GTA. It may therefore supervise the operators' obligations included in the TSM Regulation.

Regarding supervision of the application of the TSM Regulation, the European Commission, in the 2023 Commission Report, points out differences in the application of this Regulation, highlighting the main factors.

The Regulation gave NRAs powers to ensure that its objectives are met. Since the Regulation entered into force, NRAs' decisions taken against internet access service providers have been challenged in court in eight Member States. In the vast majority of cases, courts' decisions have confirmed the NRAs' decisions. In its 2020 guidelines, BEREC noted that there are three types of actions which NRAs can pursue to monitor and ensure compliance: (i) supervising or monitoring the application of different requirements; (ii) enforcement; and (iii) reporting on findings from the monitoring exercises. The imposition of any requirements and measures should be assessed based on their effectiveness, necessity and proportionality.

According to the study, enforcement practices differ widely. Whereas some NRAs pursue multiple cases and conclude cases with formal findings or decisions, others enforce the provisions of the Regulation through informal dialogue, and others use a combination of approaches to achieve compliance. Stakeholders broadly agree that NRAs have acted in accordance with the BEREC guidelines. Views about the degree to which the guidelines have led to more consistent practices across Member States are more varied, with consumer rights organisations agreeing strongly with this statement, while internet access service providers are more neutral on this point.

Madrid, 30 June 2026

APPENDIX I
GLOSSARY OF TERMS

- **BEREC.** Body of European Regulators for Electronic Communications

- **CAP (Content Access Provider)**

  ENISA (European Union Agency for Cybersecurity)

- **IPTV (Internet Protocol Television)**

- **ISP (Internet Service Provider)**

- **NN.** Net neutrality

- **NRA.** National Regulatory Authority. Every Member State invests an NRA with the administrative powers provided for in EU regulations.

- **TELECOMMUNICATIONS SINGLE MARKET REGULATION or TSM REGULATION.** Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union

- **SETELECO.** State Secretariat for Telecommunications and Digital Infrastructure, at the Ministry of Digital Transformation and the Civil Service

APPENDIX II

SUMMARY OF SETELECO CRITERIA ON PRACTICES CONCERNING NET NEUTRALITY

1. ZERO RATING

SETELECO criteria regarding zero rating offers:

In accordance with the rulings handed down by the CJEU and the BEREC Guidelines on the matter, zero rating offers are no longer admissible.

2. FREE CHOICE OF ROUTER

SETELECO criteria regarding offers analysed that could limit end-users' free choice of router:

Some operators consider it essential to only install routers supplied by them. This practice is not considered to be in conflict with the legislation provided that the end-user may later install a router of their choice. To this end, the operator must provide the end-user with the configuration parameters they request.

3. RESTRICTIONS ON DATA SHARING WITH OTHER DEVICES (TETHERING)

SETELECO criteria regarding offers analysed that limit data sharing with devices not directly connected to the network (tethering):

Offers that could limit data sharing with devices not directly connected to the network have been considered to be in conflict with the TSM Regulation. Such restrictions would only be admissible if used as temporary and exceptional traffic management measure for tackling network congestion.

4. RESTRICTIONS ON USE OF MULTI-SIM CARDS

SETELECO criteria regarding multi-SIM card offers:

In limited mobile data plans, there are no grounds for restricting the use of multi-SIM cards. Any restriction would be considered to be in violation of the TSM Regulation.

In unlimited data plans, it is admissible for ISPs to impose restrictions for the purpose of preventing users from converting one line into multiple lines by linking a different card to each device. However, the data consumptions of each secondary device used should be treated equally.

5. RESTRICTIONS ON USE OF SIM CARDS ON CERTAIN DEVICES

SETELECO criteria regarding offers analysed that restrict the use of SIM cards in certain devices:

Offers limiting the use of SIM cards in certain devices have been considered to be in conflict with the TSM Regulation. Such limitations are only admissible in the case of devices used to resell telephone traffic or to produce irregular or undue traffic.

6. TRAFFIC COMPRESSION TECHNIQUES

SETELECO criteria regarding offers that include traffic compression techniques:

The new BEREC Guidelines largely restrict the possibility of using image compression techniques such as ABR.

7. BLOCKING PORTS FOR SECURITY REASONS

SETELECO criteria regarding offers that include port blocking for security reasons:

SETELECO considers that these offers, and the practice of port blocking for security reasons, i.e. to prevent spam or malware, are in line with the TSM Regulation.

8. PRIORITIZATION OF TRAFFIC IN CASE OF NETWORK CONGESTION

SETELECO criteria regarding offers that prioritize traffic on the grounds of network congestion:

Traffic management measures aimed at preventing network congestion are considered to be in accordance with the TSM Regulation provided that they meet the following requirements:

- **They are applied to complete categories of traffic and do not discriminate between applications, services or content within them**
- **They are conceived as temporary and exceptional measures in the terms of Article 3 of the TSM Regulation**

APPENDIX III
REFERENCE DOCUMENTS

No.	DOCUMENT TITLE	ABBREVIATED TITLE USED IN THIS REPORT	WEBSITE
1	BEREC Guidelines on the Implementation of the Open Internet Regulation BEREC, June 2022	2022 BEREC Guidelines	https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-the-implementation-of-the-open-internet-regulation-0
2	BEREC Guidelines on the Implementation of the Open Internet Regulation BEREC, June 2020	2020 BEREC Guidelines	https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/*Guidelines*/9277-berec-*Guidelines*-on-the-implementation-of-the-open-internet-regulation
3	BEREC opinion for the evaluation of the application of Regulation and the BEREC Net Neutrality Guidelines BEREC, December 2018	2018 BEREC Opinion	https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/8317-berec-opinion-for-the-evaluation-of-the-application-of-regulation-eu-20152120-and-the-berec-net-neutrality-*Guidelines*
		2022 BEREC Opinion	https://www.berec.europa.eu/en/document-categories/berec/opinions/berec-opinion-for-the-evaluation-of-the-application-of-regulation-eu-2015-2120

4	BEREC opinion for the evaluation of the application of Regulation and the BEREC Net Neutrality Guidelines BEREC, December 2022		
5	Guideline on assessing security measures on the context of article 3(3) of the open Internet Regulation ENISA, December 2018	2018 ENISA Guidelines	https://www.enisa.europa.eu/publications/*Guideline*-on-assessing-security-measures-in-the-context-of-article-3-3-of-the-open-internet-regulation
6	Report from the Commission to the European Parliament and the Council on the implementation of the open internet access provisions of Regulation (EU) 2015/2120 European Commission, 28 April 2023	2023 Commission Report	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023DC0233
7	Report from the Commission to the European Parliament and the Council on the implementation of the open internet access provisions of Regulation (EU) 2015/2120 European Commission, 30 April 2019	2019 Commission Report	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0203
8	The effects of zero rating	OCDE *ZERO RATING* 2019	https://www.oecd.org/en/publications/the-effects-of-zero-rating_6eefc666-en.html

	OCDE, July 2019		
9	BEREC Report on the implementation of Regulation (EU) 2015/2120, and BEREC Net neutrality Guidelines BEREC, October 2019	2019 BEREC Report	https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8840-report-on-the-implementation-of-regulation-eu-20152120-and-berec-net-neutrality-*Guidelines*
10	Public consultation on the Draft BEREC Guidelines on the implementation of the open Internet Regulation BEREC, 10 October 2019	2019 BEREC Public consultation	https://berec.europa.eu/eng/document_register/subject_matter/berec/public_consultations/8849-public-consultation-on-the-draft-berec-*Guidelines*-on-the-implementation-of-the-open-internet-regulation
11	Report on the implementation of Regulation (EU) 2015/2120 and BEREC Net Neutrality Guidelines, October 2020	2020 BEREC Report	https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/9440-berec-report-on-the-implementation-of-regulation-eu-20152120-and-berec-net-neutrality-*Guidelines*
12	Report on the implementation of Regulation (EU) 2015/2120 and BEREC Open Internet Guidelines 2021, September 2021	2021 BEREC Report	https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/10034-berec-report-on-the-implementation-of-regulation-eu-20152120-and-berec-open-internet-*Guidelines*-2021
13		2022 BEREC Report	https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-implementation-of-the-open-internet-regulation-2022

	Report on the implementation of Regulation (EU) 2015/2120 and BEREC Open Internet Guidelines 2022, October 2022		
14	Report on the implementation of Regulation (EU) 2015/2120 and BEREC Open Internet Guidelines 2022, October 2023	2023 BEREC Report	https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-implementation-of-the-open-internet-regulation
15	Report on the implementation of Regulation (EU) 2015/2120 and BEREC Open Internet Guidelines 2022, October 2024	2024 BEREC Report	https://www.berec.europa.eu/en/all-documents/berec/reports/berec-report-on-the-implementation-of-the-open-internet-regulation
16	Report on the implementation of Regulation (EU) 2015/2120 and BEREC Open Internet Guidelines 2022, October 2025	2025 BEREC Report	https://www.berec.europa.eu/en/all-documents/berec/reports/berec-report-on-the-implementation-of-the-open-internet-regulation-0
17	Judgments on the Open Internet Regulation by the Court of Justice of the European Union	CJEU Rulings	Judgment of 15 September 2020 regarding the cases C-807/18 and C-39/19 Judgment of 2 September 2021 regarding the case C-854/19 Judgment of 2 September 2021 regarding the case C-5/20 Judgment of 2 September 2021 regarding the case C-34/20