PANORAMIC

TELECOMS & MEDIA

Italy

LEXOLOGY

Telecoms & Media

Contributing Editors

Alexander Brown, David Trapp, Edoardo Tedeschi, Matteo Susta-, Christopher Götz, Martin Gramsch, Eva Stephan and Raza Rizvi

Simmons & Simmons

Generated on: June 11, 2026

Contents

Telecoms & Media

Contributors

Italy

Simmons & Simmons

Edoardo Tedeschi edoardo.tedeschi@simmons-simmons.com
Matteo Susta matteo.susta@simmons-simmons.com
Lidia Letterelli lidia.letterelli@simmons-simmons.com

COMMUNICATIONS POLICY

Regulatory and institutional structure

Summarise the regulatory framework for the communications sector. Do any foreign ownership restrictions apply to communications services?

For the purposes of this chapter, references to the Electronic Communications Code (Legislative Decree No. 259/2003) should be understood as subsequently amended (eg, by Legislative Decree No. 207/2021 and Legislative Decree No. 48/2024). Furthermore, on portability, reference should also be made to Law Decree No. 48 of 11 April 2025 (converted by Law No. 80 of 9 June 2025), Law No. 193 of 16 December 2024 (Annual Law for the Market and Competition 2023), Legislative Decree No. 138 of 2024 (the NIS2 Decree), and Law No. 132 of 23 September 2025 (AI governance and investments).

In addition, sector-specific requirements affecting public-sector cloud procurement and (where applicable) data location or sovereignty constraints should be read together with the National Cybersecurity Agency (ACN) Regulation for Digital Infrastructures and Cloud Services for Public Administrations (adopted on 27 June 2024).

The primary legislation governing the communication sector in Italy is still the Electronic Communications Code, which implemented the EU regulatory framework and regulates the electronic communications networks and services, the authorisation of electronic communications networks and services, the interconnection of electronic networks and user rights, and aims at:

- updating and harmonising the regulation of electronic communications networks and services;
- promoting the efficient, effective and coordinated use of spectrum and the development of very high-capacity networks;
- creating a favourable environment for investment and co-investment in very high-capacity networks;
- facilitating the access of operators into electronic communications markets and promoting competition;
- facilitating the access of users to electronic communications services and strengthening the protections provided for them; and
- defining the competencies of the regulatory and administrative authorities of the sector, and in particular the Italian Communications Authority, the Ministry of Enterprises and Made in Italy (formerly the Ministry of Economic Development), and the newly established National Cybersecurity Agency.

More recently, Law Decree No. 48/2025 introduced new provisions regarding methods for user identification and established penalties for non-compliance.

Law Decree No. 48 of 11 April 2025, converted without amendments into Law No. 80 of 9 June 2025, significantly strengthened customer identification requirements for mobile telephony services under the Electronic Communications Code. In particular, it amended article 98-undetricies by introducing stricter due diligence obligations, requiring that, where the customer is a non-EU national, the operator or authorised reseller must obtain and retain

a copy of a valid residence permit or, alternatively, a valid passport, travel document or identity document. Furthermore, in cases where such documentation cannot be provided due to theft or loss, the operator or reseller is required to acquire a copy of the corresponding police report.

In addition, the Law Decree reinforced the sanctioning framework by amending article 30 of the Electronic Communications Code (introducing new paragraph 19-bis), which provides for the temporary closure of business premises for a period ranging from five to 30 days in the event of a breach of the identification obligations by authorised SIM resellers.

The Annual Law for the Market and Competition 2023 amended the Electronic Communications Code by adding additional provisions to article 98-duodecies, paragraph 1-bis, concerning the use of data contained in the mobile number portability database (including restrictions on the use of such information for commercial offering purposes). The amendment requires the Italian Communications Authority (AGCOM) to update, within 120 days, its mobile number portability regulation (currently set out in AGCOM Resolution No. 147/11/CIR) by introducing monitoring and supervisory measures aimed at ensuring the database is used consistently with the statutory restrictions; AGCOM must also publish an annual report on the results of such monitoring and oversight activities. Article 41 of the NIS2 Decree regulates the transitional regime and made the necessary repeals for the implementation of the NIS2 Directive on cybersecurity, establishing the legal framework to ensure an orderly transition to the new provisions. In particular, article 2, paragraph 1, h), article 30, paragraph 26, and articles 40 and 41 of the Electronic Communications Code were repealed.

Legislative Decree No. 48/2024 contains corrective provisions to the 2003 Electronic Communication Code, aiming to simplify the implementation of electronic communication infrastructures and the adaptation to technological innovation.

The main amendments concern:

- the introduction of the definitions of Access Point and Mac Address (media access control address);
- the introduction of the concept of Certified Start of Activity Report (SCIA), to allow a homogeneous recognition of the legal authorisation schemes;
- the introduction of textual amendments to the original provisions regarding the market entry and distribution;
- the introduction of some changes in the area of access to local radio-frequency networks; and
- the introduction of some new rules for the activation of sim cards (including references to numbering resources, blocking of foreign numbers, identification of mobile phone users).

Legislative Decree No. 70/2003 (the E-Commerce Decree) provides for the rules governing liability of internet service providers (ie, access, caching and hosting providers).

Legislative Decree No. 196/2003 (the Data Protection Code) provides specific rules concerning the protection of personal data processed by operators in the context of provision of electronic communications services, in addition to the provisions laid down in Regulation (EU) 2016/679 (the General Data Protection Regulation (GDPR)).

Moreover, the Italian Communications Authority (AGCOM) issues resolutions as secondary legislation containing detailed rules in the offering of electronic communication services and networks. Indeed, AGCOM, established by Law No. 249/1997, is a regulatory agency designed to actively promote the integration between the telecommunication and media markets and to supervise and monitor the markets.

The Data Protection Authority issues resolutions containing specific obligations for operators in the storage, processing and use of personal data information.

The Ministry of Enterprises and Made in Italy (the Ministry) is in charge, inter alia, of issuing authorisations and allocating the spectrum.

A general authorisation is required to offer electronic communications services in Italy. Such authorisation can be issued only to:

- entities with a permanent establishment in Italy or a country within the European Economic Area;
- member states of the World Trade Organization; and
- countries granting Italian citizens reciprocal rights of access to the relevant telecoms activity (article 11 of the Electronic Communications Amending Law).

Such general authorisation must be obtained for every single service offered, by submitting an application drawn up in accordance with Annex 14 to the Electronic Communications Amending Law, exclusively through the website of the Ministry's SIDFORS platform.

Requests for general authorisations to operate phone centres, internet points, fax and data-processing centre services do not have to be submitted through the SIDFORS portal but directly to the competent territorial inspectorate.

Law stated - 5 May 2026

Authorisation/licensing regime

Describe the authorisation or licensing regime.

Under article 11 of the Electronic Communications Amending Law, an operator that intends to provide electronic communications networks and services or to establish and operate network equipment at a point of presence in Italy shall apply with the Ministry for the issuance of a general authorisation that is required to offer electronic communications services in Italy.

The request must describe the services to be rendered and provide identification data about the applicant.

Starting from the filing of the relevant request, the operator is immediately entitled to run the activity. However, the Ministry has a 60-day term (from filing) to deny the authorisation. If the Ministry does not respond within this deadline, the authorisation is definitively issued.

General authorisations have a maximum validity of 20 years and may be renewed.

All operators holding a general authorisation are obliged to register with the Register for Communications Operators kept by AGCOM.

General authorisations are subject to payment of an annual contribution to the Ministry, whose amount is indicated in the Electronic Communication Code based on the service currently provided by the operator and the relevant extension thereof.

Law stated - 5 May 2026

Flexibility in spectrum use

Do spectrum licences generally specify the permitted use or is permitted use (fully or partly) unrestricted? Is licensed spectrum tradable or assignable?

The spectrum licences specify the permitted spectrum use. Under article 14 of the 2003 Electronic Communications Code, the Ministry prepares the master plan for the use of spectrum licences, while AGCOM is in charge of the allocation plan.

The most up-to-date master plan is Ordinary Supplement No. 35, adopted by Ministerial Decree dated 31 August 2022 and published in Italian Official Gazette No. 214 on 13 September 2022. It provides the principles for the allocation of the frequencies between zero GHz and 3,000GHz to each type of service (eg, fixed, mobile, satellite or radio navigation), the authorities to which the frequencies shall be required (eg, the Ministry and the Ministry of Defence) and the frequency bands and (if any) the international provision applicable.

Individual rights of spectrum use are granted within the limits set out in the master plan, and any holders of such rights shall be compliant with the spectrum use allocated.

Law stated - 5 May 2026

Ex-ante regulatory obligations

Which communications markets and segments are subject to ex-ante regulation? What remedies may be imposed?

The electronic communications sector subject to ex ante regulation has been defined through a series of EU Recommendations. Commission Recommendation No. 879 of 17 December 2007 originally identified two main groups of relevant markets:

- markets for fixed networks (eg, services for access to new generation networks); and
- markets for interconnection services on fixed and mobile networks (eg, interconnection services on fixed networks).

Commission Recommendation No. 710 of 9 October 2014 subsequently replaced the 2007 Recommendation, modifying the number and list of markets susceptible to ex ante regulation. In particular, the 2014 Recommendation included fixed and mobile call-termination markets in the list, as well as wholesale broadband access markets.

In December 2020, the European Commission adopted Commission Recommendation (EU) 2020/2245 on relevant product and service markets susceptible to ex ante regulation, which replaced the 2014 Recommendation and constitutes the currently applicable framework at EU level. The 2020 Recommendation focuses primarily on two wholesale connectivity markets (wholesale local access and wholesale access to dedicated capacity), while fixed

and mobile call termination markets are no longer listed (without prejudice to national market findings based on the three-criteria test).

The European Commission, under article 64 of Directive (EU) 2018/1972, which establishes the European Electronic Communications Code (EECC), periodically reviews electronic communications markets that may be subject to ex ante regulation, updating the "Recommendation" on relevant markets. National regulatory authorities (NRAs) are required to analyse these markets and, in some cases, can identify additional markets for regulation. NRAs must also review markets not included in the Recommendation if they are already regulated based on previous market analyses.

AGCOM, under Legislative Decree No. 207 of 8 November 2021, which transposes the EECC, conducts periodic market analyses to identify relevant markets at the national level, check for the presence of companies with significant market power, and determine if ex ante regulatory obligations should be imposed.

On 1 November 2022, Regulation (EU) 2022/1925 (the Digital Markets Act (DMA)) came into force. It regulates the activities of major digital platforms in the EU market and it applies to gatekeepers, namely, companies offering online intermediation services (including search engines, social networks, messaging and video sharing).

The DMA introduces an ex ante approach whereby specific and circumscribed obligations are imposed on the operators of platforms qualified as gatekeepers.

Law stated - 5 May 2026

Structural or functional separation

Is there a legal basis for requiring structural or functional separation between an operator's network and service activities? Has structural or functional separation been introduced or is it being contemplated?

Under article 17 of the Electronic Communications Amending Law, companies with exclusive or special rights for public communication network installation or communication services provision – in Italy or even abroad – shall provide networks or electronic communication services accessible to the public only through their subsidiaries or affiliated companies (eg, structural separation). This limitation does not apply to companies that generate an annual turnover of less than €50 million with the provision of electronic communication networks or services in the European Union.

Functional separation is instead provided by article 88 of the Electronic Communications Amending Law as an exceptional measure to be implemented if AGCOM assesses that other available remedies have failed to achieve effective competition. If AGCOM intends to impose a functional separation, it shall notify its proposal to the European Commission, explaining the grounds of such proposal.

Law stated - 5 May 2026

Universal service obligations and financing

Outline any universal service obligations. How is provision of these services financed?

The services that must be made available to end users and must be provided by all operators as universal service obligations are:

- access to end users from a fixed workstation (article 96 of the Electronic Communications Amending Law); and
- special measures for disabled and low-income users (article 95 of the Electronic Communications Amending Law).

AGCOM identifies one or more undertakings in charge of providing the universal service at an accessible price.

If AGCOM finds that the provision of the universal services by the identified undertaking results in an unfair burden to the latter upon the undertaking's request, it will share the net costs deriving from the provision of the universal services among providers of electronic communications networks and services using the ad hoc fund established by the Ministry (article 98-ter of the Electronic Communications Amending Law).

Law stated - 5 May 2026

Number allocation and portability

Describe the number allocation scheme and number portability regime in your jurisdiction.

With Resolution No. 274/07/CONS (article 6 et seq), AGCOM has set the standards for activation and migration of fixed number procedures and pure number portability (it will take place without being accompanied by the transfer of physical access resources).

Under article 98-octies decies of the Electronic Communications Amending Law, users have the right to change operator for mobile phone, voice and data services, while keeping their own mobile number (mobile number portability). The relevant inter-operator procedures are regulated by Resolution No. 339/18/CONS. The user is not actively involved in the transfer procedure. It is simply requested to subscribe to an offer with a new operator and communicate to the latter the transfer code. Thus, the user shall not even communicate the withdrawal to the former operator as the new operator is in charge of dealing with the transfer procedure, including liaising with the former operator to terminate the user's contractual relationship.

With Resolution No. 86/21/CIR, AGCOM introduced new verification obligations for the operator involved in the portability procedure to avoid the risk of fraud with SIM card replacement (called SIM Swap) against consumers. Such obligations came into force on 14 November 2022.

In parallel within the unsolicited communications and telemarketing practice, AGCOM has recently strengthened the regulatory framework governing the use of numbering resources and the presentation of the calling line identification (CLI), with the aim of addressing the increasing phenomena of spam calls and caller ID spoofing.

In particular, with Resolution No. 21/26/CIR of 14 April 2026, AGCOM updated the National Numbering Plan (PNN) and its implementing provisions in relation to the identification of the call originator and the authorised use of numbering resources. The resolution introduces a set of binding obligations designed to ensure the traceability and authenticity of the CLI used in voice calls and messaging services.

Under the updated framework, the electronic communications service provider responsible for originating a communication is expressly required to ensure the correctness of the CLI. Where the CLI is generated by the customer, the provider must verify that it corresponds to a numbering resource actually assigned to the originating line and to the relevant end user. In the absence of such correspondence, the provider is required to block the origination of the communication, whether a call or a message. These obligations apply irrespective of the technology used and are intended to prevent the illegitimate use of existing national numbering ranges through spoofing techniques.

Resolution No. 21/26/CIR also clarifies the categories of numbering that may be used as CLI. Such categories include geographic numbers, mobile and personal numbers, numbering for emergency services, public utility services and harmonised European social value services, customer care numbers, numbering for call-collect services, numbering dedicated to SMS or MMS and data transmission, as well as alphanumeric identifiers (alias), in accordance with AGCOM's specific implementing rules. Any use of CLI outside these categories is prohibited.

The use of numbering assigned to emergency services, public utility services and harmonised European social value services as CLI is permitted exclusively in accordance with the instructions issued by the relevant assigning public authority. Unauthorised use of such numbering as CLI may trigger blocking measures at network level.

Law stated - 5 May 2026

Customer terms and conditions

Are customer terms and conditions in the communications sector subject to specific rules?

Consumers are generally protected by Italian Legislative Decree No. 206/2005 (the Consumer Code) both from a contractual point of view (including off-premises agreements) and against unfair business-to-consumer commercial practices (including teleselling practices).

Specific rules are further provided by the E-Commerce Decree (implementing EU Directive 2000/31/EC) on information society services and electronic commerce, which, among others, includes specific provisions on the information to be provided to consumers when dealing with electronic agreements.

Also, the Electronic Communications Code provides for specific terms and conditions to be included in communications contracts, such as the services provided, the minimum service level, and the procedures used by the company for measuring network traffic.

EU Directive 2019/2161 (Omnibus Directive) was implemented in Italy on 18 March 2023 with Legislative Decree No. 26/2023, which entered into force on 2 April 2023, introducing new consumer protection measures in the Consumer Code including, inter alia, higher penalties for companies and widening the cases of unfair commercial practices. In particular,

with specific reference to e-commerce, the legislation introduced by Legislative Decree No. 26/2023 imposes the obligation to:

- clearly indicate, in marketplaces, the entity – professional or private – that offers products for sale, bearing in mind that, in the case of private individuals, consumer protection rules will not apply;
- to inform about the main parameters governing the classification of products, whenever the possibility of searching for products offered by different professionals is offered (this obligation, however, does not apply to providers of online search engines); and
- to ensure the reliability of product reviews.

In the energy sector, general consumer protection principles have been significantly reinforced by Decree-Law No. 19 of 28 February 2025 (the Decreto Bollette), converted into Law No. 60 of 24 April 2025. The new framework introduced targeted amendments to the Consumer Code aimed at curbing aggressive or opaque marketing practices by electricity and gas suppliers.

The legislation imposes stricter requirements on commercial communications, with particular emphasis on teleselling, telemarketing and distance-selling techniques. Energy operators are now required to ensure full transparency of promotional content, robust traceability of consumer consent and contractual confirmations through durable media.

These rules significantly limit the scope of permissible marketing strategies in the sector and expose operators — as well as digital intermediaries involved in customer acquisition or lead-generation activities — to increased enforcement risk. Breaches may result in substantial administrative fines and corrective interventions by consumer and energy regulators.

The updated numbering discipline is part of a broader regulatory strategy aimed at countering aggressive teleselling and telemarketing practices, which AGCOM has frequently associated with fraudulent activities and systematic CLI spoofing. According to the Authority, such practices undermine transparency, user trust and the effectiveness of sector-specific consumer protection tools, including data protection rules and the Public Register of Oppositions.

The enhanced control over the presentation and validation of the CLI, combined with network-level blocking obligations, is therefore intended to reinforce the traceability of communications and reduce the circulation of deceptive calls originating from manipulated national or international numbers.

Law stated - 5 May 2026

Net neutrality

Are there limits on an internet service provider's freedom to control or prioritise the type or source of data that it delivers? Are there any other specific regulations or guidelines on net neutrality?

Net neutrality is regarded as a fundamental principle recognised by AGCOM to ensure democratic internet service provision. Net neutrality is regulated by Regulation

(EU) 2015/2120, and in Italy, the competent Authority issued specific Resolution No. 348/18/CONS concerning the net-neutrality regulation. Several legislative discussions have resulted in the Declaration of Internet Rights of 14 July 2015 approved by the Italian parliament, a document consisting of 14 sections and conceived as a guideline to drive an evolutionary interpretation of the existing provisions and to serve for any legislative developments.

Article 4 of Law No. 167/2017 raised the maximum penalty that can be imposed by AGCOM, in the case of a violation of net neutrality, to a limit of €2.5 million.

In compliance with the Body of European Regulators for Electronic Communications' guidelines, AGCOM published the 2024 report including the activities carried out concerning net neutrality. The report highlights AGCOM's commitment to ensuring open and non-discriminatory Internet access, in line with Regulation (EU) 2015/2120.

The document outlines AGCOM's monitoring and regulatory activities, including oversight of internet service provider practices, transparency in traffic management, and protection of user rights. It also describes international cooperation with the Body of European Regulators for Electronic Communications, an organisation that brings together national regulatory authorities from across Europe to promote consistent regulation of electronic communications. The report emphasises the importance of regulation in fostering a fair and innovative digital environment.

The Federal Communications Commission's decision of 14 December 2017 to repeal net neutrality rules in the United States did not have a direct impact on the Italian regulatory framework. In April 2024, the FCC adopted the Safeguarding and Securing the Open Internet Order, reinstating open-internet protections; however, the US Court of Appeals for the Sixth Circuit subsequently vacated the order in its entirety in January 2025, holding that the FCC lacked the requisite statutory authority. These developments in the US regulatory landscape have not prompted any legislative response in Italy, where net neutrality remains firmly anchored to Regulation (EU) 2015/2120 and to AGCOM Resolution No. 348/18/CONS. Separately, the deployment of 5G networks raises novel questions as to whether certain forms of traffic differentiation — such as network slicing — can be reconciled with the principle of equal treatment of traffic enshrined in the EU framework.

Law stated - 5 May 2026

Platform regulation

Is there specific legislation or regulation in place, and have there been any enforcement initiatives relating to digital platforms?

While Italy has no single standalone domestic platform act, digital platform obligations are primarily driven by directly applicable EU rules, notably Regulation (EU) 2022/2065 (Digital Services Act (DSA)), which applies to providers of intermediary services as of 17 February 2024; at national level, AGCOM acts as the Digital Services Coordinator (DSC).

In any case, the following legislation may apply to various aspects of the digital platforms:

- the e-commerce regulation provided by the E-Commerce Decree;
- the Consumer Code and the data protection rules provided by the GDPR; and

- the Data Protection Code.

Moreover, the Italian Competition Law (Law No. 118/2022) introduced a provision specifically referred to digital platforms consisting in a relative presumption of economic dependence in the event that an enterprise uses the intermediation services provided by a digital platform that plays a decisive role in reaching end users or suppliers, including in terms of network effects or data availability.

In addition, Regulation (EU) 2019/1150 on platform-to-business relationships (the P2B Regulation), in force in EU member states since July 2020, outlines the relationship between business users of online intermediation services (marketplaces) and search engines.

The purpose of this Regulation is to guarantee greater transparency in the contractual terms applied to business users by, among others, the big players of the network. The target of the Regulation is the relationship of dependence that business users have on these large online players to offer their goods and services to consumers, which indirectly affects consumers who may not be able to enjoy balanced offers. The Regulation is directly applicable in EU member states and, so far, Italy has issued no specific rules regarding its implementation. By 13 January 2022, and subsequently every three years thereafter, the European Commission shall evaluate this Regulation and report to the European Parliament, the European Council and the European Economic and Social Committee.

In Italy, the enforcement of the P2B Regulation is entrusted to AGCOM pursuant to article 1, paragraph 515 of Law No. 178/2020 (Budget Law 2021). AGCOM exercises supervisory and sanctioning powers in relation to the transparency obligations imposed by the P2B Regulation on providers of online intermediation services and online search engines operating in the Italian market.

In the exercise of its functions, AGCOM has adopted guidelines and conducted monitoring activities aimed at verifying compliance with the P2B Regulation's requirements, including the obligation to provide transparent and intelligible terms and conditions for business users, to establish accessible internal complaint-handling mechanisms and to identify suitable mediators. AGCOM's enforcement activity has focused, in particular, on the clarity of ranking parameters and the adequacy of notification procedures in the event of restriction, suspension or termination of business users' accounts. While the P2B Regulation does not, in itself, impose registration or financial obligations on platform providers, it should be noted that providers of online intermediation services operating in Italy may independently be subject to additional regulatory requirements under domestic law. Depending on the nature and scope of the services provided, such requirements may include registration with sector-specific registers maintained by AGCOM (such as the Register for Communications Operators) and the payment of regulatory contributions, pursuant to the applicable provisions of the Electronic Communications Code and AGCOM's resolutions. Accordingly, operators subject to the P2B Regulation are advised to assess their compliance obligations in the broader context of the Italian regulatory framework, taking into account the potential applicability of sector-specific registration, contribution and transparency requirements that may arise independently of the P2B Regulation itself. On 27 October 2022, the DMA was published in the EU's Official Journal. The DMA regulates the activities of major digital platforms in the EU market, and it applies to gatekeepers, namely, companies offering online intermediation services (including search engines, social networks, messaging and video sharing). Eligible gatekeepers are suppliers that:

- have a size that has an impact on the internal market (assessed on the basis of turnover and capitalisation thresholds);
- are in control of important access for business users to end consumers; and
- have an established and durable position.

The designation as gatekeepers is made by the EU Commission, following a notification from the companies concerned, or acting ex officio. Under the DMA, specific and circumscribed obligations are imposed on the operators of platforms qualified as gatekeepers.

The DSA governs digital platforms, imposing specific obligations to ensure online safety, user protection and transparency in practices. Platforms must remove illegal content, provide clear information about moderation and advertising policies, and ensure reporting mechanisms for users. In Italy, AGCOM is responsible for implementing the DSA, which also covers digital intermediary platforms (such as social media and search engines). The DSA requires platforms to protect minors, prevent the spread of harmful content, and provide quick remedies in the case of user rights violations. The Act applies to all providers of intermediary services, as of 17 February 2024. A key provision of this framework is the creation of "trusted flaggers", as outlined in article 22 of the DSA. These are organisations recognised for their specialised knowledge in identifying illegal online content. Due to their reliability, the DSA grants preferential treatment to notifications they send to online platforms under article 16. Recently, on 22 January 2025, AGCOM appointed the first trusted flagger in Italy, the company Argo Business Solutions Srl. The qualification was granted in relation to issues concerning the violation of intellectual property rights and other commercial rights, as well as combating online scams and fraud. As a trusted flagger, Argo Business Solutions will be responsible for reporting illegal content to online platforms, which will be required to assess such reports promptly and effectively.

Following the introduction of national measures aimed at strengthening the protection of minors in the digital environment, AGCOM adopted regulatory provisions requiring the implementation of age-verification mechanisms for access to online content intended for adults. These measures were issued in the context of domestic legislation adopted in the aftermath of Decree-Law No. 123/2023 (Caivano Decree). However, in a series of judgments delivered on 7 April 2026, the Regional Administrative Court of Lazio partially annulled AGCOM's regulatory framework insofar as it automatically extended age-verification obligations to service providers established in other EU member states. The Court held that such an extension infringed the procedural safeguards laid down in Directive 2000/31/EC (the E-Commerce Directive), in particular the principle of the country of origin and the obligation to activate prior cooperation and notification mechanisms at EU level before imposing restrictive measures on cross-border service providers.

While age-verification obligations remain applicable to providers established in Italy, the decisions significantly curtail the extraterritorial reach of AGCOM's enforcement powers. The case illustrates the structural tension between national digital policy initiatives and the constraints imposed by EU internal market law.

Law stated - 5 May 2026

Next-Generation-Access (NGA) networks

Are there specific regulatory obligations applicable to NGA networks? Is there a government financial scheme to promote basic broadband or NGA broadband penetration?

Since 2015, Italy has been executing the ultra-broadband strategic plan (UBP) to develop an ultra-broadband network across all Italian territory and create a public telecommunications infrastructure in coherence with the purposes of the European Digital Agenda. The Ministry acts through its in-house company (Infratel Italia SpA) whose mission is to implement the infrastructure development schemes throughout the country, with a particular focus on the development of an ultra-broadband network and Wi-Fi public-services connection.

The UBP is part of the wider Italian Ultra-Broadband Strategy – approved by the government in March 2015 – which intends to reduce the existing market and infrastructure gap through the creation of conditions that are more favourable to the integrated development of fixed and mobile telecommunications infrastructure. Such strategy represents the reference national framework for any public initiative supporting the development of ultra-broadband networks in Italy.

The strategy is implemented through state aid (national and EU funds alike), approved by the European Commission. Moreover, on 11 February 2016, the Council of Ministers and the Conference of the Regions approved the "Framework agreement on the developing of the NGA as European target 2020", allocating €3 billion to the project, subdividing the funds to the regions, according to their population, and strengthening the management of the project.

The intervention is intended to build a publicly owned network that will be made available to all operators willing to provide services in favour of the population and undertakings.

On 6 July 2023, the Interministerial Committee for Digital Transition approved the Ultra Broadband (BUL) Strategy 2023–2026. This strategy aims to address critical gaps in the BUL value chain, identified through a detailed analysis of the current state of ultra-high capacity network creation and dissemination in Italy. The primary goal of the BUL Strategy is to bridge these gaps, ensuring seamless integration and enhancement of digital infrastructure across the country. By doing so, the strategy seeks to significantly strengthen the Italian telecommunications sector, providing a robust foundation for sustained economic growth. The anticipated economic benefits are substantial, with an estimated increase in gross domestic product of €96.5 billion between 2020 and 2025, and €180.5 billion between 2020 and 2030. The strategy outlines several key interventions:

- enhancing public administration skills and sector research and development;
- strengthening monitoring, programming and planning activities;
- building and enhancing network infrastructure;
- increasing network efficiency and resilience; and
- supporting demand and increasing take-up.

Law stated - 5 May 2026

Data protection

Is there a specific data protection regime applicable to the communications sector?

The data protection framework applicable to the electronic communications sector in Italy is based on a multi-layered regulatory structure. The primary sources are:

- the GDPR, which establishes the general framework for the processing of personal data;
- the Data Protection Code, as substantially amended by Legislative Decree No. 101/2018, which contains sector-specific provisions applicable to the processing of personal data in the context of the provision of publicly available electronic communications services; and
- Directive 2002/58/EC (the ePrivacy Directive), as transposed into Italian law through Title X (articles 121 to 132-quater) of the Data Protection Code.

In particular, articles 121 to 132-quater of the Data Protection Code apply to the processing of personal data in connection with the provision of electronic communications services accessible to the public on public communications networks, addressing matters such as confidentiality of communications, traffic and location data, cookies and similar tracking technologies, unsolicited communications and data retention.

Pursuant to article 122 of the Data Protection Code, the storage of information in the terminal equipment of a user or the access to information already stored therein is permitted only on the condition that the user has provided informed consent, after receiving clear and comprehensive information in accordance with article 13 of the GDPR. This requirement does not apply to technical storage or access that is strictly necessary for the transmission of a communication over an electronic communications network, or for the provision of an information society service explicitly requested by the user. The Data Protection Authority has issued specific guidelines on the use of cookies and other tracking tools (most recently, Guidelines No. 231 of 10 June 2021), which clarify the modalities for obtaining valid consent, the requirements for cookie banners and the distinction between technical and profiling cookies.

Under article 123 of the Data Protection Code, traffic data relating to subscribers and users processed by the provider of a public communications network or a publicly available electronic communications service must be erased or anonymised when they are no longer necessary for the purpose of transmitting a communication. The provider may process traffic data to the extent and for the duration strictly necessary for billing purposes, interconnection payments and the resolution of related disputes. Furthermore, the provider may process traffic data for the purpose of marketing its own electronic communications services or providing value-added services, provided that the subscriber or user has given prior, specific and informed consent, which may be withdrawn at any time. In all cases, the processing of traffic data must be restricted to persons acting under the authority of the provider who are specifically authorised and limited to what is strictly necessary for the purposes of billing, traffic management, customer enquiries, fraud detection or the marketing of electronic communications services.

A particularly significant aspect of the Italian data protection framework applicable to the communications sector concerns data retention obligations. Article 132 of the Data Protection Code requires providers of publicly available electronic communications services

to retain telephony traffic data for 24 months and telematic (internet) traffic data for 12 months, for the purposes of detection and suppression of criminal offences. These retention periods were extended by Law No. 167/2017 (article 24) to 72 months for the most serious criminal offences (including terrorism, organised crime and other offences listed therein). The compatibility of such extended retention periods with EU law — in particular with the principles established by the Court of Justice of the European Union (CJEU) in its judgments in ***Digital Rights Ireland*** (C-293/12), ***Tele2 Sverige*** (C-203/15) and ***La Quadrature du Net*** (C-511/18) — remains a matter of ongoing legal debate. The CJEU has consistently held that general and indiscriminate retention of traffic and location data is incompatible with EU law, while targeted retention may be permissible where justified by serious threats to national security or serious crime, subject to strict proportionality requirements and effective judicial or independent administrative oversight.

Pursuant to article 125 of the Data Protection Code, where CLI is available, the provider of a publicly available electronic communications service must ensure that the calling user has the possibility, free of charge and by means of a simple function, to prevent the presentation of the CLI on a per-call basis. The called subscriber must also have the possibility, free of charge, to prevent the presentation of the CLI of incoming calls and to reject incoming calls where the calling user has prevented the presentation of the CLI. These provisions implement the requirements of the ePrivacy Directive concerning the confidentiality of communications and the rights of calling and called parties.

Under article 126 of the Data Protection Code, location data other than traffic data relating to users or subscribers of public communications networks or publicly available electronic communications services may only be processed if such data are rendered anonymous, or with the prior, specific and informed consent of the user or subscriber, to the extent and for the duration necessary for the provision of a value-added service. The consent may be withdrawn at any time. The provider must inform the user or subscriber, prior to obtaining consent, of the type of location data that will be processed, the purposes and duration of the processing, and whether the data will be transmitted to a third party for the purpose of providing the value-added service. The user or subscriber must retain the possibility of temporarily refusing the processing of location data, free of charge and by means of a simple function, each time the network is accessed or for each connection.

Article 130 of the Data Protection Code regulates unsolicited communications for the purposes of direct marketing, advertising or market research. The use of automated calling systems without human intervention, fax machines, email, SMS, MMS or any other electronic communications means for the sending of marketing material is permitted only with the prior consent of the subscriber or user (opt-in regime). A limited exception applies under article 130, paragraph 4 (soft-spam provision): where a data controller has obtained the electronic contact details of a customer in the context of a sale of a product or service, such details may be used for direct marketing of the controller's own similar products or services, provided that the customer is clearly and adequately informed at the time of collection and is given the opportunity to object, free of charge and in a simple manner, to such use both at the time of collection and on the occasion of each subsequent communication. In all cases, the sending of communications for marketing purposes must comply with the general principles of the GDPR, including the requirement of a valid legal basis, transparency and the data subject's right to object at any time.

The provisions of the GDPR apply in full to the processing of personal data carried out by providers of electronic communications services. In particular, the rights of data subjects

under articles 15 to 22 of the GDPR (including the rights of access, rectification, erasure, restriction of processing, data portability and objection) must be guaranteed by all operators. Furthermore, where the processing of personal data — particularly traffic, location or content data — is likely to result in a high risk to the rights and freedoms of natural persons, the provider is required to carry out a data protection impact assessment (DPIA) pursuant to article 35 of the GDPR prior to commencing the processing. The Data Protection Authority has identified specific categories of processing operations subject to mandatory DPIA, which include large-scale processing of location data and systematic monitoring of publicly accessible areas through electronic communications networks.

Concerning the security of processing, article 32 of the GDPR requires providers of publicly available electronic communications services to implement technical and organisational measures appropriate to the level of risk, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risks of varying likelihood and severity for the rights and freedoms of natural persons. In the electronic communications sector, such measures must ensure, in particular, that traffic data, location data and any other personal data stored, transmitted or processed through the network are protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Where the security of the service or of personal data also requires the adoption of measures relating to the network infrastructure, the provider of the publicly available electronic communications service must adopt such measures jointly with the provider of the public communications network. In the event of failure to reach an agreement, either provider may refer the matter to AGCOM for resolution. In addition, pursuant to articles 33 and 34 of the GDPR, providers must notify the Data Protection Authority of any personal data breach without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the breach is likely to result in a high risk, the Data Protection Authority must also communicate the breach to the affected data subjects without undue delay. The Data Protection Code further specifies, at article 132-bis, the obligation for providers of any personal data breach without undue delay and, where feasible, within 72 hours of becoming aware of it, unless data breaches, including the breach is unlikely to result in a risk to the rights and freedoms natural persons. Where the breach is likely to result in a high risk the provider must also communicate the breach to the affected data subjects without undue delay. The Data Protection Code further specifies, article 132-bis, obligation for providers publicly available electronic communications services to maintain an updated inventory data breaches including circumstances, effects and remedial actions taken, to enable the Data Protection Authority to verify compliance.

Furthermore, pursuant to article 132-bis of the Data Protection Code, the provider of a publicly available electronic communications service must inform subscribers and, where possible, users — using clear, appropriate and adequate language, with particular attention to the category and age group of the subscriber, especially in the case of minors — if there is a particular risk of a breach of network security. Where the risk falls outside the scope of the measures that the provider is required to adopt, the provider must indicate all possible remedies available to the user and the relative presumable costs. The provider must also communicate such information to the Data Protection Authority and AGCOM. These obligations complement the general transparency and accountability requirements under

the GDPR and are designed to ensure that end users are adequately informed of risks that may affect the confidentiality and integrity of their communications.

In the area of direct marketing and telemarketing, a key instrument of the Italian regulatory framework is the Public Register of Oppositions (Registro Pubblico delle Opposizioni (RPO)). Italian Presidential Decree No. 26 of 27 January 2022, which repealed and replaced the previous Presidential Decree No. 178/2010, significantly expanded the scope and functioning of the RPO. The RPO is a public registry administered by the Fondazione Ugo Bordoni under the supervision of the Ministry, in which subscribers and data subjects may register their telephone numbers — including, since the entry into force of Presidential Decree No. 26/2022, mobile telephone numbers — in order to oppose the receipt of telephone calls for marketing purposes.

Registration in the RPO has the effect of revoking all previously granted consents to the processing of the subscriber's or data subject's contact data for marketing purposes by telephone, regardless of the manner or time at which such consents were originally provided. The revocation operates erga omnes, unless the subscriber or data subject expressly limits the opposition to one or more specific operators.

The extension of the RPO to mobile telephone numbers — previously excluded under the 2010 regime — represents a significant development, as it substantially broadens the scope of protection available to data subjects against unsolicited marketing communications in the electronic communications sector.

Any entity intending to carry out telemarketing activities is required to register with the RPO and to consult the register prior to initiating any marketing campaign. The entity must submit to the RPO the list of telephone numbers it intends to contact for marketing purposes.

Upon receipt of the request, the RPO returns to the requesting entity, within 24 hours, an updated list from which the numbers registered in the RPO have been removed. The entity is prohibited from contacting the numbers so excluded.

The cleared list returned by the RPO is valid for a maximum period of 15 days from the date of its generation, after which the entity must carry out a new consultation to obtain an updated list. This mechanism ensures that the RPO remains continuously updated and that the rights of subscribers who register or modify their preferences in the interim are promptly respected.

As noted above, registration in the RPO operates as a withdrawal of consent within the meaning of article 7(3) of the GDPR. Accordingly, from the moment of registration, any operator that has not obtained a new, specific and informed consent from the data subject after the date of registration is prohibited from contacting the registered number for marketing purposes.

The subscriber or data subject retains the right to limit the scope of the opposition, excluding from its effects one or more specific operators or categories of operators. In such cases, the operators expressly excluded from the opposition may continue to contact the subscriber for marketing purposes, subject to compliance with all other applicable data protection requirements.

The Data Protection Authority approved the Code of Conduct for telemarketing and teleselling activities (Codice di condotta per le attività di telemarketing e teleselling) with resolution No. 70 of 9 March 2023, pursuant to article 40 of the GDPR. The Code was subsequently published in the Official Gazette and became effective following the

accreditation of the Monitoring Body (Organismo di Monitoraggio (OdM)) by the Data Protection Authority with resolution No. 148 of 7 March 2024 (Official Gazette No. 73 of 27 March 2024). The OdM is an independent body entrusted with verifying adherents' compliance with the Code, handling complaints and promoting best practices in the sector. Adherence to the Code is voluntary but, once undertaken, becomes binding on the adhering entity.

Entities adhering to the Code undertake to adopt specific measures to ensure the lawfulness and transparency of personal data processing throughout the entire telemarketing and teleselling chain. Such measures include, inter alia:

- the collection of specific, granular and documented consents for each distinct processing purpose (marketing, profiling, communication to third parties);
- the provision of clear, precise and complete information to the persons contacted regarding the purposes for which their data are processed and the identity of the data controller;
- the implementation of effective mechanisms for the exercise of data subjects' exercise of data subjects' rights, including the right to object;
- the adoption of contractual safeguards in relations with sub-contractors and list brokers; and
- the establishment of internal audit and compliance procedures.

Adherence to the Code may be taken into account by the Data Protection Authority as a mitigating factor in the context of enforcement proceedings, in accordance with article 40(4) of the GDPR.

Law stated - 5 May 2026

Cybersecurity

Is there specific legislation or regulation in place concerning cybersecurity or network security in your jurisdiction?

From a local standpoint, two main pieces of legislation on cybersecurity are to be noted:

- NIS2 framework; and
- Cybersecurity Perimeter.

On 27 December 2022, the NIS2 Directive, which updates and succeeds Directive (EU) 2016/1148 on the security of network and information systems (the NIS Directive), was published in the EU's Official Journal. The NIS2 Directive was transposed into Italian law by the NIS2 Decree, published in the Official Gazette on 1 October 2024 and in force since 16 October 2024. The NIS2 Decree repealed the previous Legislative Decree No. 65/2018 (which had transposed the original NIS Directive) and establishes a comprehensive framework aimed at ensuring a high common level of cybersecurity at the national level.

The main innovation of the NIS2 Directive is its wide area of application, which is extended to medium and large companies operating in further sectors such as, inter alia:

- cloud computing;

- data centres;
- content delivery network providers;
- electronic communication services; and
- electronic communication networks.

The scope of the Directive — and of the NIS2 Decree — extends to the entire information and communications technology (ICT) infrastructure of the entities concerned. Entities are categorised as either essential (***soggetti essenziali***) or important (***soggetti importanti***) based on the criticality of their activities, the sector in which they operate and their size. Under the NIS2 Decree, the classification is carried out by the ACN, which maintains and periodically updates the list of entities falling within the scope of the legislation. Entities subject to the NIS2 Decree are required to register on the dedicated digital platform established by ACN, providing the information necessary for their identification and classification. The initial registration deadline was set at 28 February 2025, with ACN subsequently notifying each registered entity of its classification as essential or important by 31 March 2025.

The entities concerned are required to adopt appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of their network and information systems. Under articles 23 to 25 of the NIS2 Decree, such measures must include, inter alia, policies on risk analysis and information system security, incident handling procedures, business continuity and crisis management arrangements, supply chain security measures, security in network and information systems acquisition, development and maintenance, policies and procedures for the use of cryptography and encryption, human resources security, access control policies and asset management. The governing bodies (***organi di amministrazione e direzione***) of the entities concerned bear direct responsibility for approving and overseeing the implementation of cybersecurity risk management measures and are required to undergo specific cybersecurity training.

The NIS2 Directive also envisages new stringent reporting requirements in the event of a cyber incident to be fulfilled by notifying the cybersecurity incident response team (CSIRT) of all incidents likely to cause impacts of a "significant" nature.

Different from the past, where reporting had to be done "without undue delay" (see the NIS Directive), the NIS2 Directive provides for a more circumscribed, comprehensive and timely reporting process. In this sense, it provides for:

- an early warning period of within 24 hours from the knowledge of the incident (the sending of the "early warning");
- a notification within 72 hours of knowledge of the incident, updating – if necessary – the information in the early warning; and
- a final report within one month from the transmission of the notification, completing the reporting process.

The NIS2 Decree designates the ACN as the national competent authority and single point of contact for NIS2 matters, and confirms CSIRT Italia — operating within ACN — as the national computer security incident response team. The ACN is entrusted with supervisory, enforcement and sanctioning powers, including the authority to conduct inspections, audits and security scans, and to issue binding instructions to non-compliant entities. The NIS2 Decree also establishes a structured sanctioning regime: essential entities may be subject to

administrative fines of up to €10 million or 2% of total worldwide annual turnover (whichever is higher), while important entities may be subject to fines of up to €7 million or 1.4% of total worldwide annual turnover (whichever is higher). In addition, the ACN may impose accessory sanctions, including the temporary suspension of certifications or authorisations and, in the most serious cases, the temporary prohibition on the exercise of managerial functions by the natural persons responsible for the breach.

The NIS2 Decree provides for a phased implementation timeline. While the registration obligations on the ACN platform applied from 1 January 2025 (with the initial deadline of 28 February 2025), the substantive cybersecurity risk management and incident reporting obligations will become fully enforceable from 1 October 2026, in accordance with the transitional provisions set out in article 42 of the NIS2 Decree. During the interim period, entities already subject to the previous NIS framework (Legislative Decree No. 65/2018) remain bound by the obligations thereunder, to the extent compatible with the new provisions. The ACN is expected to adopt further implementing measures and guidelines to specify the technical and procedural requirements applicable to the entities concerned.

With reference to the Cybersecurity Perimeter, five implementing decrees are provided to fully implement the architecture of the Perimeter. The first implementing decree was fully effective from 5 November 2020 (Presidential Decree No. 131/2020) and defines the criteria for identifying the entities included in the Perimeter and the obligations imposed on them to safeguard national security. The list of entities included in the Perimeter has already been drawn up, with about 100 entities involved, but was not published for national security reasons.

Nonetheless, the sectors in which to identify, as a matter of priority, in relation to public and private entities carrying out functions with a significant impact on national security include, among others, telecommunications, digital services and critical technologies.

Furthermore, Presidential Decree No. 131/2020 imposes several obligations on the entities within the Perimeter to ensure a high level of security.

First, entities must prepare, and annually update, the list of their ICT assets and must then identify the ICT assets needed to perform the essential function or service, to:

- assess the impact of an incident on the ICT asset, in terms of its operability and the compromise of data availability, integrity or confidentiality; and
- assess dependencies with other networks, information systems, IT services or physical infrastructures belonging to other subjects.

Finally, entities must identify the ICT assets that, in the event of an incident, would cause the total interruption of the essential function or service.

The second implementing Decree on notifications of incidents affecting networks, information systems and information services, as well as security measures, is Presidential Decree No. 54/2021. This Decree identifies the procedures, modalities and terms by which the National Assessment and Certification Centre (CVCN) and the Assessment Centres of the Ministries of Interior and Defence (CV) carry out assessments on the acquisition, by the entities included in the Perimeter, of ICT technologies and software – including 5G technology – that could present vulnerabilities and therefore expose them to cyber risks.

The latter Decree provides that, before the launch of award procedures or the conclusion of supply contracts, entities included in the Perimeter must notify the CVCN or the CV. Subsequently, the procedure is divided into three phases:

- preliminary assessments;
- preparation for the execution of tests; and
- execution of hardware and software tests.

The third implementing Decree, fully effective from 8 May 2021 (Presidential Decree No. 54/2021 of 5 February 2021), focuses on the procedures and terms for assessments by the CVCN and the CVs on products being acquired by entities included in the Perimeter.

The latter Decree also establishes the criteria for identifying the supply objects falling within the categories to which the assessment procedure applies.

Indeed, the categories of ICT goods, systems and services subject to the assessment by the CVCN or the VCs are identified based on the execution or performance of the following functions:

- switching or protection against intrusion and detection of cyber threats in a network, including the application of security policies;
- command, control and implementation in an industrial control network;
- monitoring and configuration control of an electronic communication network;
- network security concerning the availability, authenticity, integrity or confidentiality of services offered or data stored, transmitted or processed;
- authentication and allocation of the resources of an electronic communication network; and
- implementation of an IT service through the configuration of an existing software program or the development, in part or in full, of a new software program, constituting the application part relevant to the provision of the IT service itself.

The Decree of the President of the Council of Ministers, 15 June 2021, was the fourth implementing the Perimeter, identified the categories of networks, information systems and IT services for which it will be necessary to notify the CVCN.

The entities included in the Perimeter will notify the commencement of a technology acquisition procedure together with a risk assessment.

The fifth implementing Decree – Decree of the President of the Council of Ministers, 18 May 2022, No. 92, defined the criteria for the accreditation of laboratories responsible for verifying the security conditions in the procurement of products, processes and services for networks, information systems and IT services.

In addition to the above, Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (the Cyber Resilience Act (CRA)) introduces mandatory cybersecurity requirements applicable to hardware and software products placed on the EU market. The CRA imposes obligations on manufacturers, importers and distributors throughout the product lifecycle, including vulnerability handling, security updates and conformity assessment procedures. Although the CRA does not specifically target the electronic communications sector, its scope encompasses a broad range of

connected devices and software — including network equipment, internet-of-things devices and embedded systems — that are widely deployed in telecommunications infrastructures. The CRA entered into force on 10 December 2024, with the main product obligations becoming applicable from 11 December 2027. In Italy, the designation of the national market surveillance authority for the purposes of the CRA is expected to involve the ACN in coordination with the Ministry.

Furthermore, Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (the Digital Operational Resilience Act (DORA)), which has applied since 17 January 2025, is also relevant to the communications sector insofar as providers of electronic communications networks and services, cloud computing providers and data centre operators may qualify as critical ICT third-party service providers designated by the European Supervisory Authorities under article 31 of DORA. Entities so designated are subject to direct oversight by the Lead Overseer and must comply with specific requirements concerning, inter alia, ICT risk management, incident reporting, resilience testing and information-sharing arrangements. Accordingly, telecommunications operators and digital infrastructure providers that supply ICT services to financial entities should assess whether their activities fall within the scope of DORA's oversight framework and, where applicable, ensure compliance with the relevant obligations.

In addition, Directive (EU) 2022/2557 on the resilience of critical entities (the CER Directive), which complements the NIS2 Directive by addressing the physical and operational resilience of entities providing essential services, was transposed into Italian law by Legislative Decree No. 134 of 4 September 2024. The CER framework applies to critical entities operating in sectors listed in the Annex to the Directive, which include, inter alia, digital infrastructure. Under the Italian implementing decree, the Presidency of the Council of Ministers is responsible for adopting the national strategy for the resilience of critical entities and for designating the competent authorities. Critical entities identified under the CER framework are required to carry out risk assessments, adopt appropriate technical, security and organisational measures to ensure their resilience, and notify significant incidents to the competent authority. The CER Directive and the NIS2 Directive are designed to operate in a complementary manner: while NIS2 addresses cybersecurity risks, the CER framework covers a broader range of threats — including natural hazards, terrorist attacks, insider threats and sabotage — that may affect the continuity of essential services provided through digital and communications infrastructures.

Law stated - 5 May 2026

Big data

Is there specific legislation or regulation in place, and have there been any enforcement initiatives in your jurisdiction, addressing the legal challenges raised by big data?

On 7 October 2024, Legislative Decree No. 144 was published in the Official Gazette, aligning national regulations with the provisions of Regulation (EU) 2022/868 (the Data Governance Act). The Decree came into effect on 25 October 2024.

The Agency for Digital Italy (AgID) has been designated as the competent authority for managing the notification procedure for data intermediation services and for registering data

altruism organisations. Additionally, AgID is expected to work in close and loyal cooperation with the following authorities: the National Cybersecurity Agency (ACN), the Competition and Market Authority (AGCM), and the Data Protection Authority (Garante). To facilitate this, AgID can enter into specific, non-onerous collaboration agreements with these authorities.

Regarding sanctions, AgID is authorised to impose administrative fines ranging from a minimum of €10,000 to a maximum of €100,000, or, for companies, up to 6% of the total worldwide annual turnover of the previous financial year. Big data often includes personal data and, in many cases, it is not possible to separate these data from non-personal data; therefore, as highlighted by the Data Protection Authority in the fact-finding survey on big data of February 2020, the privacy risks derived from the use of big data are different:

- the processing of personal data outside the purposes for which it was collected;
- the use of incorrect or outdated information;
- discrimination or prejudice against certain individuals or groups resulting from the application of certain profiling algorithms; and
- the processing of personal data above what is necessary to process them.

In addition, Regulation (EU) 2023/2854 (the Data Act) has become largely applicable as of 12 September 2025. The Data Act introduces new rights for users (including businesses) to access and port certain data generated through the use of connected products and related services, and enables data sharing with third parties designated by the user, subject to safeguards (including trade secrets and data protection compliance). It also sets obligations for providers of data processing services (including cloud and other 'as-a-service' models) to facilitate switching and interoperability and to reduce provider lock-in.

Law stated - 5 May 2026

Data localisation

Are there any laws or regulations that require data to be stored locally in the jurisdiction?

As a general principle, Regulation (EU) 2018/1807 on the free flow of non-personal data in the European Union prohibits member states from imposing data localisation requirements unless justified on grounds of public security, in compliance with the principle of proportionality. Within this framework, certain sector-specific localisation requirements are nonetheless provided by:

- the Regulation for Digital Infrastructures and Cloud Services for Public Administration issued by the ACN, which provides that in some cases the data must be stored within European territory;
- the Cybersecurity Perimeter;
- the ACN Regulation for Digital Infrastructures and Cloud Services for Public Administrations (adopted on 27 June 2024 under article 33-septies(4) of Decree-Law No. 179/2012, as transposed), which sets classification rules for public-sector data and digital services (ordinary, critical or strategic) and establishes qualification or adequacy requirements for cloud services and infrastructures used by public

administrations; depending on classification, this framework may entail EU or EEA location and sovereignty-related constraints for data and service deliver; and

- DORA, as applicable to financial entities and their supply chain.

Any data localisation requirement imposed under Italian law must therefore be assessed for compatibility with Regulation (EU) 2018/1807 and, where personal data are involved, with the provisions of the GDPR governing international data transfers.

Certain limitations may apply concerning specific types of data.

By way of example, under article 39 of Presidential Decree No. 633/1972 (relating to the value added tax applicable to the sale of goods and services), any accounting document shall be retained through electronic archives and stored in a foreign country only to the extent that there are reciprocal assistance rights.

Law stated - 5 May 2026

Key trends and expected changes

Summarise the key emerging trends and hot topics in communications regulation in your jurisdiction.

The Italian communications sector is undergoing a period of profound transformation, driven by the convergence of major EU regulatory initiatives, national legislative reforms and rapid technological evolution. The following paragraphs outline the principal trends shaping the regulatory and market landscape.

A first area of significant development concerns the regulation of AI. Regulation (EU) 2024/1689 (the AI Act), which entered into force on 1 August 2024, establishes a harmonised EU framework for the development, placing on the market and use of AI systems, based on a risk-based classification approach. The AI Act's prohibitions on unacceptable-risk AI practices have applied since 2 February 2025, while the obligations for providers of general-purpose AI models apply from 2 August 2025 and the full regime for high-risk AI systems will become applicable from 2 August 2026. At the national level, Italy adopted Law No. 132 of 23 September 2025, which establishes national principles and sector-specific provisions on the development and use of AI, to be interpreted and applied consistently with the AI Act. The law creates a national governance system for AI, coordinated by the Presidency of the Council of Ministers, and establishes a dedicated fund of €1 billion for investments in AI, cybersecurity, quantum technologies and 5G telecommunications. Specific areas of application are regulated, including the labour market, data protection, minors' access to AI systems and cybersecurity, with measures to ensure inclusion and accessibility for persons with disabilities. AgID and ACN are entrusted with the development of support tools, including regulatory sandboxes pursuant to article 57 of the AI Act, and initiatives aimed at promoting innovation, competitiveness and the responsible adoption of AI technologies. In the context of AI and personal data protection, Garante has been at the forefront of enforcement activity at EU level. On 30 March 2023, the Garante ordered a temporary limitation on the processing of personal data of data subjects established in Italy by OpenAI in connection with the ChatGPT service, citing deficiencies in transparency and information obligations, concerns regarding the legal basis for the processing of personal data for algorithmic training purposes, and the absence of adequate age-verification

safeguards for minors. At EU level, the European Data Protection Board established a dedicated task force to foster cooperation among national data protection authorities in relation to ChatGPT. On 29 January 2024, the Garante notified breaches of data protection law to OpenAI, and the investigation remains ongoing. The Garante has also opened separate proceedings concerning other generative AI services and has concluded a public consultation on data scraping for the purposes of training AI algorithms, although no formal guidelines have been published to date.

A second key trend concerns the development of ultra-broadband infrastructure and the deployment of 5G networks. The Inter-Ministerial Committee for Digital Transition, established by Decree-Law No. 22 of 1 March 2021, coordinates Italy's ultra-broadband strategy Towards the Gigabit Society, approved on 25 May 2021, which encompasses various interventions including the Italian 5G plan (for which €2,020 million of National Recovery and Resilience Plan resources have been allocated). On 6 July 2023, the Interministerial Committee approved the BUL Strategy 2023–2026, aimed at addressing critical gaps in the ultra-high capacity network value chain. With Resolution No. 67/22/CONS of 3 March 2022, AGCOM adopted guidelines to identify the conditions of wholesale access to ultra-broadband networks receiving public contribution, including specific provisions for 5G networks. The progressive rollout of 5G infrastructure raises novel regulatory questions, including the reconciliation of network slicing and traffic differentiation techniques with the principle of equal treatment of traffic enshrined in Regulation (EU) 2015/2120 on net neutrality.

The Italian telecommunications market is undergoing a significant phase of structural consolidation. The spin-off of TIM's fixed network assets to FiberCop SpA, acquired by KKR with a minority stake held by the Italian Ministry of Economy and Finance, has fundamentally reshaped the wholesale access market. The merger between Fastweb and Vodafone Italia, approved with remedies by the AGCM in December 2024, has further reduced the number of infrastructure-based operators. These transactions raise important questions regarding the future competitive dynamics of both the fixed and mobile markets, the effectiveness of existing wholesale access remedies and the potential need for AGCOM to reassess its market analyses in light of the changed market structure.

A third area of rapid regulatory evolution is cybersecurity. The transposition of the NIS2 Directive by the NIS2 Decree has significantly expanded the scope of cybersecurity obligations applicable to entities operating in the communications sector, with substantive risk management and incident reporting obligations becoming fully enforceable from 1 October 2026. In parallel, the CRA introduces mandatory cybersecurity requirements for products with digital elements placed on the EU market, with main obligations applicable from 11 December 2027. DORA, applicable since 17 January 2025, is relevant to telecommunications operators and digital infrastructure providers insofar as they may qualify as critical ICT third-party service providers subject to direct oversight by the European Supervisory Authorities. The CER Directive, transposed by Legislative Decree No. 134/2024, complements the NIS2 framework by addressing physical and operational resilience of entities providing essential services, including digital infrastructure. The cumulative effect of these instruments is to create a multi-layered cybersecurity compliance framework that will require significant organisational and technical adaptation by operators in the communications sector.

From a regulatory and policy perspective, AGCOM has expressly adopted a proportionate and incremental approach to addressing the phenomenon of caller ID spoofing, taking into

account both the technical complexity of the issue and the potential economic impact of certain end-to-end authentication solutions. In Resolution No. 21/26/CIR of 14 April 2026, the Authority acknowledged that some internationally discussed technical standards for call authentication, such as STIR/SHAKEN, may entail significant implementation costs and operational burdens, particularly in cross-border traffic scenarios, and may not be immediately suitable for uniform application within the Italian numbering ecosystem.

Against this background, AGCOM has prioritised regulatory interventions focused on strengthening upstream controls over the assignment and use of numbering resources, enhancing contractual accountability along the electronic communications service chain and introducing targeted network-level blocking obligations for non-compliant traffic. Central to this approach is the reinforcement of the link between the CLI and the actual originator of the communication, with a view to improving traceability, auditability and enforcement effectiveness, while avoiding the imposition of generalised obligations on legitimate communications.

In parallel, AGCOM has established a dedicated technical working group tasked with developing further technical, regulatory and operational measures to prevent the illegitimate generation and use of CLI, including with regard to mobile numbering, sub-assignment practices and messaging services. The Authority has indicated that any future measures will be guided by principles of gradual implementation, proportionality and measurability, with particular attention to high-risk contexts such as large-scale teleselling and telemarketing activities. This approach reflects AGCOM's intention to reconcile effective user protection and trust in electronic communications with the need to preserve operational flexibility and cost efficiency for market operators.

The regulation of digital platforms continues to evolve rapidly. The DSA, fully applicable since 17 February 2024, imposes graduated obligations on providers of intermediary services, with AGCOM designated as the national DSC. AGCOM has commenced its supervisory activities, including the appointment of the first trusted flagger in Italy in January 2025. The DMA introduces ex ante obligations on designated gatekeepers, with enforcement proceedings already initiated by the European Commission against several major platforms. At the national level, the interplay between the DSA and DMA framework and existing domestic provisions — including the P2B Regulation, enforced in Italy by AGCOM, and the economic dependence provisions introduced by Law No. 118/2022 — creates a complex and evolving regulatory environment for platform operators active in the Italian market.

- Data governance and data sharing represent a further area of significant regulatory development. The Data Act, largely applicable since 12 September 2025, introduces new rights for users to access and port data generated through the use of connected products and related services, and imposes obligations on providers of data processing services to facilitate switching and interoperability. The Data Governance Act, implemented in Italy by Legislative Decree No. 144/2024, establishes a framework for data intermediation services and data altruism organisations, with AgID designated as the competent national authority. These instruments, together with the GDPR and the sector-specific provisions of the Data Protection Code, are progressively reshaping the regulatory framework applicable to the collection, processing and sharing of data in the communications sector.
- The protection of minors in the digital environment remains a prominent regulatory priority. AGCOM has adopted regulatory provisions requiring the implementation

of age-verification mechanisms for access to online content intended for adults, in the context of domestic legislation adopted in the aftermath of the Caivano Decree. However, in a series of judgments delivered on 7 April 2026, the Regional Administrative Court of Lazio partially annulled AGCOM's regulatory framework insofar as it automatically extended age-verification obligations to service providers established in other EU member states, holding that such extension infringed the procedural safeguards laid down in Directive 2000/31/EC (the E-Commerce Directive). While age-verification obligations remain applicable to providers established in Italy, the decisions illustrate the structural tension between national digital policy initiatives and the constraints imposed by EU internal market law. The topic is expected to remain at the centre of regulatory debate, also in light of the DSA's provisions on the protection of minors and the forthcoming implementing measures under the AI Act concerning AI systems interacting with minors.

- Finally, the themes of digital sovereignty, cloud regulation and foreign investment screening are increasingly relevant to the communications sector. The ACN Regulation for Digital Infrastructures and Cloud Services for Public Administrations, adopted on 27 June 2024, establishes classification rules for public-sector data and digital services and imposes qualification and adequacy requirements for cloud services and infrastructures used by public administrations, with potential EU or EEA data location constraints depending on the classification level. In parallel, the golden power framework (Law Decree No. 21/2012, as subsequently amended and extended) continues to apply to foreign direct investments in the communications and media sectors, with the scope of notifiable transactions having been progressively broadened in recent years to encompass 5G technology, cloud computing and data storage activities. These developments reflect a broader trend towards the assertion of national strategic interests in the governance of critical digital infrastructures.

Law stated - 5 May 2026

MEDIA

Regulatory and institutional structure

Summarise the regulatory framework for the media sector in your jurisdiction.

Audio-visual media sectors are mainly governed by Legislative Decree No. 208/2021, namely, the Consolidated Law on Audio-visual Media Services (AVMS Code), which has implemented the Audio-Visual Media Service Directive (Directive (EU) 2018/1808 amending Directive (EU) 2010/13/EU (AVMS Directive) in Italy.

Decree No. 208 of 8 November 2021 reorganised the provisions of the Consolidated Audiovisual Media Act (CAMA), referred to in Legislative Decree No. 177 of 31 July 2005.

One of the aims of Decree No. 208/2021 is to adopt the national plan for the allocation of radio frequencies in analogue technique, taking into account the degree of development of radio broadcasting in digital technique.

Additionally, the main subject matter of Decree No. 208/2021 is the provisions on audiovisual media services, such as:

- the transmission of:
- television programmes, both linear and on-demand;
- radio programmes; and
- data programmes, including those with conditional access; and
- the provision of associated interactive services and conditional access services on any broadcasting platform, including audiovisual commercial communications and video-sharing platform services.

Decree No. 208/2021 applies to audiovisual and radio media service providers and radio concessionaires operating in Italy, which are those that:

- have their head office in Italy and editorial decisions on the audiovisual media service are taken in Italy;
- have their head office in Italy and editorial decisions on the audiovisual media service provided are taken in another EU member state or a third country, if a significant part of the persons employed in the performance of the audiovisual or radio media service activity linked to the programmes operate within Italian territory;
- despite having its head office in another EU member state or a third country, editorial decisions on the audiovisual media service provided are taken in Italy and a significant part of the persons employed in the performance of the audiovisual or radio media service activity are linked to the programmes operate within Italian territory;
- a significant part of the workforce involved in the pursuit of the audiovisual media service activity relating to the programmes operates both in Italy and in another EU member state if its head office is in Italy; and
- if it started its activity in Italy in compliance with the national legal system, maintaining over time a stable and effective link with the Italian economy.

To the already-existing prohibitions against incitement to hate and violence, the prohibition to commit public provocation to terrorist offences has been added. Moreover, Decree No. 208/2021 aims to ensure adequate protection of human dignity and minors in relation to audiovisual content and commercial communications by sharing platforms.

On 17 April 2024, Legislative Decree No. 50/2024 was published in the Official Gazette as a reform to Legislative Decree No. 208/2021. The system of programming and investment quotas in European and Italian works has been simplified, reducing obligations for European on-demand services (from 20% to 16% investment and from 3.5% to 3% of revenue). On the other side, the quota for recent Italian-language works (produced within the last five years) has been increased from 50% to 70%. In addition, a new Interinstitutional Advisory Committee has been established, replacing the previous Media and Minors Committee, with a mandate to provide consultation and promote media and digital literacy.

Legislative Decree No. 44/2010 has simplified the provision of linear services, regulated the provision of non-linear services (eg, download and on-demand services), and introduced

some limits concerning advertisement crowding, as well as specific dispositions for the protection of European works.

Legislative Decree No. 181/2021, which has implemented Directive (EU) 789/2019 and amended certain rules concerning television rebroadcasting rights.

Legislative Decree No. 177/2021, which has implemented Directive (EU) 790/2019 on copyright and related rights in the Digital Single Market.

The two main institutional bodies in Italy for the media sector are the Italian Communications Authority (AGCOM) and the Ministry of Enterprises and Made in Italy (the Ministry). AGCOM is vested in all powers and responsibility for development and policymaking activities in connection with the provision of radio and audiovisual services. The Ministry has the power, among others, to grant licences, general authorisations and spectrum.

Law stated - 5 May 2026

Ownership restrictions

Do any foreign ownership restrictions apply to media services? Is the ownership or control of broadcasters otherwise restricted? Are there any regulations in relation to the cross-ownership of media companies, including radio, television and newspapers?

CAMA was aimed at protecting the media market as well as ensuring pluralism in the provision of relevant audiovisual services through the implementation of certain ownership restrictions for broadcasters. Article 51 of Decree No. 208/2021 replaces article 43 of CAMA and contains the provisions related to the protection of pluralism fixing certain thresholds of incomes, and taking into account the changed market conditions with the increasing presence of multinational platforms. Such restrictions should be applied regardless of the nationality of the broadcasters.

In its judgment of 3 September 2020 in ***Vivendi SA v Autorità per le Garanzie nelle Comunicazioni*** (Case C-719/18), the Court of Justice of the European Union (CJEU) found article 43 of CAMA contrary to EU law, because, although it is based on the general interest of protecting pluralism in the media, it entails a restriction of the freedom of establishment within the meaning of article 49 of the Treaty on the Functioning of the European Union.

To be compliant with the principles of such judgment, Decree No. 208/2021 provides an obligation for the companies to notify when thresholds are exceeded and a consequent detailed investigation carried out by AGCOM to verify the impairment of pluralism as set out in the provisions.

Concerning the cross-ownership of media companies, article 51, paragraph 3(c) of Decree No. 208/2021 provides for companies whose revenues exceed 8% of the total revenues of the integrated system of communications and that, at the same time, have or acquire stakeholdings in companies publishing daily newspapers, except for companies publishing daily newspapers distributed exclusively by electronic means, to formally notify AGCOM, within 15 days from the deed transferring ownership or from the conclusion of the preliminary agreement between the parties of such context that constitute indications of a position of significant market power potentially detrimental to pluralism. AGCOM is in charge of issuing the authorisation for the transaction.

A further restriction concerns the acquisition by EU and non-EU parties of participation in media companies. Indeed, the golden power discipline also applies to such transactions (ie, foreign direct investment). The golden power regulation (Law Decree No. 21/2012) is a set of rules according to which the Italian government may exercise some veto rights in relation to certain corporate resolutions and or to share purchase agreements in specific economic sectors or for assets of specific sectors,.

Law stated - 5 May 2026

Licensing requirements

What are the licensing requirements for broadcasting, including the fees payable and the timescale for the necessary authorisations?

Under Decision No. 353/11/CONS of AGCOM relating to the licensing of digital terrestrial radio and television broadcasting (the DTT Regulation), digital terrestrial television (DTT) network operators must have a general authorisation to operate a DTT network issued by the Ministry and must obtain the right to use the relevant radio frequency spectrum. The DTT Regulation provides for various requirements for DTT network operators, including the number of programmes to be broadcast, coverage requirements and, in particular circumstances, must-carry obligations.

Service providers must apply for a general authorisation before providing their services.

The broadcasting authorisation is issued by the Ministry for a maximum of 12 years, renewable for a successive period of equal duration upon request to be sent 30 days before the expiry date. Applications may be filed only by entities established in Italy, other EEA states or other countries applying reciprocal treatment to Italians willing to operate as broadcasters in such countries. No authorisation is required for the retransmission of programmes by broadcasters established and legitimately operating in countries that are signatories of the European Convention on Transfrontier Television. The Ministry decides within 60 days of the application.

Licences can be transferred to a third party if the latter meets the requirements provided by AGCOM's resolution governing the licence. The new licensee must communicate the transfer of the licence to the competent authority, which either authorises the assignment or communicates its own denial, based on the assignee's lack of compliance with requirements provided by the law (eg, if the assignee is based in a non-EU country that does not apply reciprocity, ie, where an Italian company could not hold an equivalent licence).

In addition, any change of control of the licensee and any assignment of licence must be notified to AGCOM. AGCOM, before authorising the deal, assesses whether the transfer may lead to the creation of a dominant position in the relevant market, which could adversely affect pluralism.

Each broadcaster shall pay a one-off fee of €7,000.

The six-year renewable authorisation procedure for satellite broadcasters (including pay-TV channels) is provided by Decision No. 127/00/CONS of AGCOM. AGCOM has 60 days to decide on any application for satellite broadcasting or cable transmission.

The satellite broadcasting and cable distribution of television programmes are subject to a one-off fee of €6,027.

Law stated - 5 May 2026

Foreign programmes and local content requirements

Are there any regulations concerning the broadcasting of foreign-produced programmes? Do the rules require a minimum amount of local content? What types of media fall outside this regime?

The broadcasting of European programmes is regulated by article 52 et seq of Decree No. 208/2021. Legislative Decree No. 50/2024 provided for the replacement of articles 52 to 57. The key changes include:

- more structured quotas for Italian works, especially recent ones and those produced by independent producers;
- increased mandatory investments, with clearly defined percentages and sub-quotas;
- guaranteed visibility for European works in on-demand catalogues (eg, dedicated sections, promotional requirements);
- enhanced role of AGCOM, with new powers for regulation, oversight and monitoring; and
- clarified economic thresholds and criteria for exemptions, ensuring proportionality and flexibility.

Linear audiovisual media service providers shall reserve for European programmes a majority proportion of their transmission time. The time used for news, sports events, games, advertising, teletext and teleshopping services shall not be taken into account.

A sub-quota of the quota envisaged for European programmes is reserved for original Italian programmes, wherever they are produced, to the extent of at least half for the concessionaire of the public radio, television and multimedia service and at least one-third for other providers of linear audiovisual media services.

In the time slot from 6pm to 11pm, the concessionaire of the public radio, television and multimedia service reserves at least 12% of broadcasting time, excluding the time allocated to news, sports events, television games, advertising, teletext and teleshopping services, for cinematographic and audiovisual works of fiction, animation, original documentaries of Italian origin, wherever produced.

Concerning foreign programmes, article 26 of Decree No. 208/2021 sets out that the authorisation released to the local broadcaster association includes the right to transmit in Italy foreign companies' programmes for a maximum of 12 hours per day. In the case of interconnection with satellite channels or foreign television broadcasters, this shall not take more than 50% of the maximum time provided for the interconnection.

Law stated - 5 May 2026

Advertising

How is broadcast media advertising regulated? Is online advertising subject to the same regulation?

Article 43 et seq of Decree No. 208/2021 regulates broadcast media advertising.

As a general rule, the advertising shall not be hidden or subliminal and shall maintain a sound level not exceeding that of the programmes. Moreover, the advertising shall be respectful of human dignity and diversity and shall not encourage behaviour that is harmful to the safety and protection of the environment. There are specific items for which advertising is forbidden, such as cigarettes, medicines and gambling, and also specific protection for minors.

Pursuant to article 44, the advertising shall be clearly identifiable and recognisable from the editorial content. News, feature films and films for television (excluding series, serials and documentaries) shall be interrupted by spots no more than every 30 minutes.

The broadcasting of advertising messages by the concessionaire of the public radio, television and multimedia service, with reference to each individual channel, the limit is set at 6%, in the time slot between 6am and 6pm and in the time slot between 6pm and midnight, and 12% in each hour. The advertising slots of pay-TV broadcasters shall not exceed a daily threshold of 15%.

Regarding radio advertisements carried out by non-public broadcasters, the hourly threshold is equal to 20% for national broadcasting, 25% for local broadcasting and 10% for national or local broadcasting by European broadcasters.

Legislative Decree No. 50/2024 also intervened in the field of advertising, extending the regulation of articles 43 et seq. to radio media service providers.

Online advertising is regulated by Legislative Decree No. 206/2005 (the Consumer Code) and Legislative Decree No. 70/2003 (the E-Commerce Decree). The Consumer Code specifically prohibits unfair trade practices, as well as misleading and aggressive marketing practices, while electronic commerce, identifies some information that the information society service provider must provide as well as the minimum requirements that any advertisement operator and any person making an online advertisement must comply with. EU Directive 2019/2161 (Omnibus Directive) was recently implemented in Italy by virtue of Legislative Decree No. 26/2023, which entered into force on 2 April 2023 and which provides for certain relevant amendments and integration to the Consumer Code, in particular providing – among other changes – for new information requirements on distance contracts, new conducts that could amount to misleading omission or practice, new sanction regime and also specific additional information requirements for the contract concluded on online marketplaces.

It is provided that – in addition to the information requirements laid down for specific goods and services – commercial communications that are part of or constitute an information society service, must include, from the first time they are sent, clearly and unambiguously, a specific statement aimed at highlighting that:

- it is a commercial communication;
- the natural or legal person on whose behalf the commercial communication is made;
- it is a promotional offer such as discounts, premiums or gifts and the conditions for accessing it; and

- it is a promotional competition or game, if allowed, and the conditions for participation.

Law stated - 5 May 2026

Must-carry obligations

Are there regulations specifying a basic package of programmes that must be carried by operators' broadcasting distribution networks? Is there a mechanism for financing the costs of such obligations?

No regulations specify a basic package of programmes that must be carried by operators' broadcasting distribution networks. However, under article 13, paragraph 4 of Decree No. 208/2021, broadcasters providing content of "particular value" shall have privileged access to the digital broadcasting network. Under Resolution No. 253/2004, contents of "particular value" at the national or a local level are those containing, inter alia, a high educational value, news and facts, socio-economic, cultural and political context, and improvement of the relationship between the citizen and the public administration.

No particular mechanism is provided to finance this kind of obligation.

Law stated - 5 May 2026

Regulation of new media content

Is new media content and its delivery regulated differently from traditional broadcast media? How?

Italian Legislative Decree No. 44/2010, deriving from EU Directive 2007/65/EC, has modified, inter alia, the provision of the audiovisual non-linear services (video on demand). It has introduced a minimum legal standard applicable to audiovisual linear services as well as to audiovisual non-linear services (eg, concerning the protection of minors and prohibition of hidden advertising). However, some specific provisions shall not apply to audiovisual non-linear services. The main example concerns advertising. Because the audience may easily avoid advertising, the daily threshold for the audiovisual non-linear advertising spots does not apply. Also, broadcasters may freely choose where to insert advertising spots.

Decree No. 208/2021, moreover, has implemented a specific regulation for video-sharing platform services. Pursuant to article 41, paragraph 7 of Decree No. 208/2021, the supervisory authority (the Communications Regulator) may restrict the free circulation of user-generated programmes and videos that are conveyed by a video-sharing platform whose provider is located in an EU member state and are directed to the Italian public, to protect the freedom of expression, prevent discrimination and hate speech.

Furthermore, Decree No. 208/2021 provides that all the providers of media services (including those through video-sharing platforms) must comply with the provisions for the protection of minors laid down in the Media and Minors Self-Regulation Code.

Law stated - 5 May 2026

Digital switchover

When is the switchover from analogue to digital broadcasting required or when did it occur? How will radio frequencies freed up by the switchover be reallocated?

The switchover procedure in Italy started in October 2008. The complete switchover from analogue to digital television in Italy occurred on 4 July 2012.

The rules and procedure for the reallocation of radio frequencies freed up by the switchover were contained in Resolution No. 550/12/CONS of AGCOM. The television frequencies have been reallocated through the principle of the "higher economic offer". In particular, the resolution provided for the allocation of 21 national multiplexes, which enable various signals to be combined into a common flow of data and the transmission of several digital terrestrial television services simultaneously. It was, in addition, provided that, at the end of the selection procedure, no operator could obtain more than five national multiplexes.

With two decisions dated 26 July 2017 (***Europa Way*** and ***Persidera***), the CJEU has ruled that the Italian switchover from analogue to digital terrestrial television was violating EU laws by failing to allocate one multiplex for each analogue channel.

Moreover, Italy had set a deadline of 30 June 2022 for the transition imposing that all TVs must gradually leave the frequencies allocated to telephone companies and can abandon Mpeg-2 video encoding and, to save bandwidth, broadcast their programmes in Mpeg-4 encoding. This procedure was completed on 21 December 2022 through the permanent switch-off of the Mpeg-2 video encoding system.

On 28 August 2024, the national multiplex Mux B, operated by the public service Rai, was effectively converted to the new DVB-T2 transmission standard and, for most of the HD channels carried, to HEVC (H.265) video coding. Rai was the first provider to switch to the new standard. During 2025, the transition to the DVB-T2 should be completed by all the operators.

Law stated - 5 May 2026

Digital formats

Does regulation restrict how broadcasters can use their spectrum?

As a general principle, broadcasters shall ensure efficient use of the radio spectrum (article 50 of Decree No. 208/2021).

This means that they shall minimise the environmental impact, avoid risks to human health, and ensure that there is no interference with other broadcasters' spectrum.

Legislative Decree No. 50/2024 introduced article 5-bis, which mandates that AGCOM adopt the National Allocation Plan for frequencies designated for digital terrestrial television services. This plan identifies several UHF band frequencies in each technical area for local planning purposes, ensuring that at least one frequency covers no less than 90% of the area's population. This measure aims to provide transmission capacity to local audiovisual media service providers and ensure that there is no interference with other broadcasters' spectrum.

Law stated - 5 May 2026

Media plurality

Is there any process for assessing or regulating media plurality (or a similar concept) in your jurisdiction? May the authorities require companies to take any steps as a result of such an assessment?

Under article 5, paragraph 1 of Decree No. 208/2021, the Italian media services system shall promote media plurality, forbidding the creation or maintenance of positions against pluralism and ensuring the transparency of broadcasters' corporate assets (eg, establishing that the same person, or persons in a relationship of control or connection between them, may not at the same time be authorised to provide digital radio media services at the national and local level). Article 51 sets out the principle that it is forbidden to create dominant positions detrimental to pluralism and it also specifies the rules for the assessment by AGCOM.

Moreover, in the case of transfer of a licence, any change of control of the licensee and any assignment of licence must be notified to AGCOM. Before authorising the deal, AGCOM assesses whether the transfer may lead to the creation of a dominant position in the relevant market, which could adversely affect pluralism.

Law stated - 5 May 2026

Key trends and expected changes

Provide a summary of key emerging trends and hot topics in media regulation in your country.

Regulation (EU) 2022/2065 (Digital Services Act (DSA)), aims to protect users online and to ensure freedom of expression. The major providers of such platforms shall be obliged to evaluate risks within their systems for public interests, fundamental rights, safety and public health. The DSA shall apply to all online intermediaries operating in the European Union, introducing graduated obligations based on the nature of the services and proportionate to the number of users, for balancing user protection with market and innovation needs.

Law stated - 5 May 2026

REGULATORY AGENCIES AND COMPETITION LAW

Regulatory agencies

Which body or bodies regulate the communications and media sectors? Is the communications regulator separate from the broadcasting or antitrust regulator? Are there mechanisms to avoid conflicting jurisdiction? Is there a specific mechanism to ensure the consistent application of competition and sectoral regulation?

The main regulators that have a role in the regulation of telecoms and audio-visual media distribution are the following.

- The Italian Communications Authority (AGCOM) is the regulator and watchdog in charge of audio-visual media and electronic communications services. AGCOM grants licences and authorisations for public broadcasting, regulates the relationship between telecoms companies and settles disputes between operators or between operators and end users. AGCOM is also in charge of preventing online copyright infringements and was appointed as the national supervisory authority under Law Decree No. 123/2023 implementing Regulation (EU) 2022/2065 (the Digital Services Act) and Regulation (EU) 2019/1150 on platform-to-business relationships (the P2B Regulation) in Italy.
- The Ministry of Enterprises and Made in Italy (the Ministry), which deals with electronic communications and audio-visual media, including, among others, allocating frequencies, the monitoring and control of the national radio spectrum, and managing the infrastructure programme for broadband. The Ministry is also in charge of the general authorisations for electronic communications networks and services, and issues the authorisations to operate digital terrestrial TV channels.

While AGCOM regulates both the communications and the broadcasting sector, the antitrust regulation pertains to the Italian Competition Authority (ICA). The ICA has exclusive competence over the enforcement of Italian competition rules in the telecoms and broadcasting sectors. AGCOM and the ICA entered into an agreement on 22 December 2016 for defining the modalities of their cooperation.

Moreover, the Data Protection Authority is the authority responsible for supervising the compliance of telecom operators with Legislative Decree No. 196/2003 (the Data Protection Code).

Last, the Italian National Cybersecurity Agency (ACN), is a government authority in charge of protecting national interests in the field of cybersecurity. Among other things, the ACN is entrusted with specific competencies in relation to the security of electronic communication networks.

Law stated - 5 May 2026

Appeal procedure

How can decisions of the regulators be challenged and on what bases?

Any act, decision or resolution of AGCOM or the ICA may be appealed, also regarding the merit of facts, to the Regional Administrative Court of Lazio by any individual or legal entity that has been directly affected by such act, decision or resolution. The Regional Administrative Court of Lazio's judgment may be appealed to the Council of State.

Law stated - 5 May 2026

Competition law developments

Describe the main competition law trends and key merger and antitrust decisions in the communications and media sectors in your jurisdiction over the past year.

The past 12 months have seen a number of potentially significant mergers and acquisitions in the communications sector, as well as important measures in the media sector. Listed below are some of the most relevant trends.

- In 2024, TIM spun off its fixed network assets, transferring them to FiberCop SpA, which was acquired by the US investment fund KKR, with a minority stake held by the Italian Ministry of Economy and Finance. The operation was authorised by the European Commission on 30 May 2024, which found no competitive concerns, given the continued presence of other active players in the national wholesale access market (Open Fiber, Fastweb and FiberCop itself). However, in December 2024, the Italian Competition Authority (AGCM) launched an investigation into the agreement between TIM and FiberCop to assess whether it contained provisions that may constitute a restrictive agreement in breach of article 101 of the Treaty on the Functioning of the European Union.
- In December 2024, the AGCM approved, with remedies, the concentration between Fastweb and Vodafone Italia, which reduced the number of infrastructure-based operators in the fixed network market to three. The transaction also increased the level of concentration in the mobile communications markets, prompting AGCOM to examine potential downstream effects.
- Another significant intervention by the AGCM concerned Wind Tre's acquisition of Opnet's business unit, which included frequencies and fixed network infrastructure used to provide fixed wireless access services. The operation, approved in May 2024, resulted in a rebalancing of spectrum holdings among mobile operators, though it did not produce any immediate competitive effects.
- On 22 January 2025, the AGCM sanctioned the Spanish company Socialwebsite SL, which operated through the website payperfan.it, for unfair commercial practices. The company was found to be selling fake social media interactions — such as followers, likes, and views — while presenting them as authentic user engagement. The AGCM deemed this conduct misleading under Italian Legislative Decree No. 206/2005 (the Consumer Code), as it was likely to distort consumers' economic decisions and harm fair competition. The decision forms part of a broader initiative by AGCOM to ensure transparency in the digital environment and combat online opinion manipulation.
- In March 2025, the AGCM sanctioned Socialwebsite SL (decision PS12799) in connection with the online sale of inauthentic social media "appreciations" (eg, followers, likes and views) marketed as genuine user engagement. In the same proceedings, AGCOM had issued an opinion to AGCM on 22 January 2025 (Delibera No. 18/25/CONS) as part of the Consumer Code cooperation mechanism for practices disseminated online.
- In April 2025, the AGCM made mandatory the commitments presented by Sky Italia regarding communications and procedures for cancelling subscriptions and downgrading, as well as the removal of packages, closing the proceedings initiated against the company without a finding of infringement (AGCM decision PS12802, Provvedimento No. 31530 of 15 April 2025).

Law stated - 5 May 2026