Metodo Giuridico
Ius et Ratio • ISSN 3103-7305
ITALIAN JOURNAL OF LAW & CASE LAW • ISSN 3103-7305
IN-DEPTH LEGAL ANALYSIS • ADMINISTRATIVE LAW & ADMINISTRATIVE JUSTICE •
13 NOVEMBER 2026

Piracy Shield Blocking Orders and AGCOM Powers over Foreign DNS and VPN Providers

The interim enforcement architecture of Law no. 93/2023 tested by the Cloudflare litigation, the allocation of supervisory powers under the Digital Services Act, and the unresolved challenges of overblocking and procedural transparency

GM Giovanni Ercole Moscarini Administrative Law & Administrative Justice 13 November 2026

Reading time 30 min

Current Legal Framework as of 12 November 2026: The consolidation of serial litigation before the Regional Administrative Court (*TAR*) of Lazio and the adoption of AGCOM Resolution no. 209/25/CONS have confirmed that cross-border technical intermediaries are fully bound by rapid blocking orders, establishing an enforcement model grounded in automated technological cooperation and the territorial criterion of harmful effects.

ABSTRACT

This article examines the **administrative enforcement framework** for combating online audiovisual piracy established by Italian Law no. 93 of 14 July 2023, as amended by Law no. 143/2024 and implemented by AGCOM Resolutions nos. 189/23/CONS, 321/23/CONS, and 209/25/CONS. The analysis investigates the doctrinal and procedural consistency of **Piracy Shield blocking orders** in light of the judgments delivered by the Regional Administrative Court (*TAR*) of Lazio (Judgments nos. 1223/2024, 14414/2024, 13201/2026, and 13202/2026) concerning the jurisdiction exercised over **foreign DNS, VPN, and CDN providers** in the Cloudflare dispute. Specifically, it scrutinizes the functional divide between Articles 9 and 56 of Regulation (EU) 2022/2065 (the **Digital Services Act**), the legal characterization of dynamic injunctions as executive acts subject to deferred adversarial review, the calculation of statutory administrative fines on the basis of **consolidated worldwide turnover** pursuant to Article 1(31) of Law no. 249/1997, and the unresolved tensions surrounding shared IP address overblocking, post-execution complaint remedies, and defensive access to technical platform logs.

Key Takeaways

- **Primary Statutory Basis and Interim Powers:** Law no. 93/2023 remedied the historical lack of statutory sanctioning powers identified by the Council of State (*Consiglio di Stato*) in Judgment no. 4993/2019, vesting AGCOM with urgent interim blocking powers to be executed within thirty minutes across networks and technical intermediaries.
- **Legal Nature of Dynamic Injunctions:** Individual blocking tickets generated through the Piracy Shield platform do not constitute autonomous challengeable administrative measures, but rather operate as executive acts updating and implementing the original interim order subject to deferred adversarial review.
- **Unresolved Challenges of Overblocking and Transparency:** The regulatory amendments enacted by Resolution no. 209/25/CONS mitigate the risk of collateral blocking on shared IP addresses and extend the administrative complaint window to ten days, while judicial case law maintains a strict bar against mass defensive access to platform technical logs.
- **Allocation of Competences under the Digital Services Act:** Article 9 DSA empowers national authorities to issue orders to act against specific items of illegal content on the basis of territorial harmful effects, whereas Article 56 DSA reserves exclusively to the Member State of establishment the supervision of systemic due-diligence obligations.
- **Fines Calculated on Worldwide Turnover:** Pecuniary administrative penalties under Article 1(31) of Law no. 249/1997 are lawfully assessed against the operator's consolidated worldwide turnover, ensuring proportionality and effective deterrence vis-à-vis foreign Big Tech intermediaries.

RESEARCH DOSSIER

JURISDICTION
Italy (Civil Law)

SUBJECT AREA
Administrative Law & Administrative Justice

SCOPE
Italian Civil Law System

Legal Principle / Editorial Headnote

Rapid blocking orders and dynamic injunctions issued by the Italian Communications Authority (AGCOM) pursuant to Article 2 of Law no. 93/2023 find their European Union legal basis in Article 9 of Regulation (EU) 2022/2065 under the territorial criterion of harmful effects, binding foreign providers of DNS, VPN, and CDN services irrespective of the Member State of establishment of their designated EU legal representative under Article 56 DSA, and lawfully supporting the assessment of pecuniary administrative sanctions under Article 1(31) of Law no. 249/1997 against the infringing undertaking's consolidated worldwide turnover.

01. THE SYSTEMATIC FRAMEWORK OF ONLINE COPYRIGHT ENFORCEMENT: FROM THE REGULATORY PROTOTYPE TO LAW NO. 93/2023

1.1 — The Genesis of Administrative Injunctive Powers and Council of State Judgment no.

4993/2019

The evolution of the statutory framework safeguarding **intellectual property rights** across electronic communications networks finds its systematic center of gravity in the conferral of far-reaching prohibitory powers upon the Italian Communications Authority (AGCOM). The operational effectiveness that currently characterizes **Piracy Shield blocking orders** is rooted in the long-standing trajectory of public-law regulation inaugurated by **Resolution no. 680/13/CONS**, whereby the independent regulatory authority first introduced a model of **administrative copyright enforcement** premised on direct intervention vis-à-vis intermediary service providers. That institutional architecture responded to the pressing need to secure swift remedial action against infringements committed in the digital environment, where the dispersion of unlawful sources and the volatility of data transmissions frequently render traditional **civil law remedies** before ordinary courts ineffective.

The lawfulness of such regulatory intervention long remained the subject of intense doctrinal and judicial debate, culminating in the landmark ruling whereby the **Council of State** (*Consiglio di Stato*) scrutinized the consistency of the administrative model with constitutional and European Union principles[1]. In upholding the validity of the Authority's **general regulatory competence** derived from **Law no. 249 of 31 July 1997** and **Legislative Decree no. 70 of 9 April 2003**, the appellate administrative court held that the provision of **administrative injunctive measures** constitutes the natural corollary for terminating unlawful conduct. Exercising such powers neither encroaches upon the constitutional **judicial reserve** nor infringes Article 21 of the Italian Constitution, inasmuch as disabling access is directed exclusively against channels disseminating unlawful materials, without curtailing freedom of expression with respect to lawful information.

Nevertheless, that same decision drew an insurmountable boundary grounded in the **principle of substantive legality** enshrined in Article 23 of the Italian Constitution and **Law no. 689 of 24 November 1981**. Specifically, the Council of State (*Consiglio di Stato*) clarified that while the Authority is empowered to issue blocking orders to protect copyrighted works, it cannot introduce **pecuniary administrative sanctions** by way of secondary regulation against non-compliant intermediaries in the absence of an explicit **primary statutory provision**. The **doctrine of implied powers** cannot be stretched so far as to establish punitive financial obligations that have not been predetermined by Parliament. That judgment exposed the structural asymmetry between the prohibitory reach of the administrative order and the weakness of its enforcement apparatus, prompting leading legal scholarship to call for comprehensive primary legislation capable of equipping the Authority with **statutorily defined coercive instruments**[D1].

1.2 — The Architecture of Law no. 93/2023 and the Legal Qualification of Interim Dynamic Orders

The enactment of **Law no. 93 of 14 July 2023** marked the definitive supersession of the prior sub-legislative regime, filling the lacuna identified by administrative case law and endowing the domestic legal order with an **express primary statutory basis**. The legislature sought to reconcile the protection of intellectual property (Articles 41 and 42 of the Italian Constitution; Article 17 of the EU Charter of Fundamental Rights) with the confidentiality of communications and the freedom of economic initiative enjoyed by technical intermediaries, shaping a system premised on **shared responsibility** across the digital ecosystem. Article 2 of the statute empowered AGCOM to order service providers — including **network access providers**, virtual private network operators, and domain name resolution providers — to disable access to unlawfully disseminated content by **blocking DNS resolution** and interrupting network traffic routing toward IP addresses *"predominantly dedicated to unlawful activities"*.

The core innovation of the reform lies in the statutory codification of **dynamic injunctions** governed by paragraphs 2 and 3 of Article 2. Faced with infringements involving live-streamed broadcasts or first-run theatrical works, the speed at which the unlawful act is consummated renders ordinary administrative procedures ineffective. Parliament therefore

designed an **expedited interim procedure** conducted *ex parte* (*inaudita altera parte*), under which the initial blocking order programmatically extends to any future domain name, subdomain, or IP address enabling redirection toward the same infringing content or materials of the same nature. This mechanism neutralizes the evasive practice known as *domain hopping*, whereby infringing streams continuously migrate across new network identifiers in order to circumvent static prohibitory orders.

From a doctrinal perspective, procedural law scholars have thoroughly examined the systematic classification of these measures, demonstrating that a dynamic order does not consist of an indeterminate sequence of separate ablative administrative acts, but rather operates as a **progressively structured command** in which the initial finding of unlawfulness serves as the legal predicate shaping **future executive obligations** incumbent upon third-party intermediaries[D2]. Effective protection hinges on the intermediary's capacity to implement the block without delay, framing the operator's conduct not as a punitive burden, but as a **duty of technical cooperation** imposed on entities which, albeit not the perpetrators of the infringement, control the infrastructure indispensable to its dissemination. Substantive legality is ultimately completed by linking non-compliance with such orders to the trigger of **statutory pecuniary penalties** under Article 5 of the Law.

02. THE OPERATIONAL FUNCTIONING OF THE PIRACY SHIELD PLATFORM AND ACCESS DISABLING WITHIN THIRTY MINUTES

2.1 — Machine-to-Machine Automation and Proportionality of the Time Limit under TAR Lazio Judgment no. 1223/2024

Implementing the mandates set forth in **Law no. 93/2023** required deploying a technological infrastructure capable of ensuring instantaneous telematic interaction among rightholders, the Regulatory Authority, and information society service providers. The **Piracy Shield platform**, established and regulated by AGCOM Resolutions nos. 189/23/CONS and 321/23/CONS, operates through an automated architecture built upon *machine-to-machine* protocols. This configuration reflects the clear legislative intent to compress procedural reaction times by requiring addressees of the order to disable domain name resolution and IP traffic routing *"within a maximum time limit of thirty minutes from notification"*. The **automation of information flows** overcomes the temporal constraints of traditional administrative fact-finding, shifting public-law oversight upstream to the accreditation of qualified reporting entities and downstream to the eventual post-execution complaint phase.

The legal and technical sustainability of such a compressed timeframe was scrutinized by the **Regional Administrative Court (*TAR*) of Lazio**, seized of actions for annulment brought by trade associations representing independent internet service providers against the implementing regulations[2]. The administrative judges dismissed the pleas alleging disproportionality and infringement of the **freedom to conduct a business**, holding that the brevity of the thirty-minute window does not amount to an arbitrary imposition, but stems directly from the inherently perishable nature of live audiovisual broadcasts. Because the unlawful streaming of a live sporting event exhausts its economic and commercial harm within a matter of hours, a **timely prohibitory measure** executed after longer delays would lack practical effectiveness and degenerate into purely symbolic relief. The judgment further reaffirmed that the administrative remedy administered by AGCOM operates concurrently rather than alternatively vis-à-vis ordinary judicial enforcement under Article 156 of the Italian Copyright Law, thereby upholding the full legitimacy of the **dual-track enforcement system**.

Legal scholarship examining the launch of the platform has emphasized that compressing the execution window compels **network intermediaries** to undertake a profound reconfiguration of their organizational structures and routing architectures, prompting operators to deploy automated blocking routines calibrated to continuously updated

blacklists[D3]. From the standpoint of administrative act theory, delegating operational execution to algorithmic processing raises delicate questions regarding the preservation of meaningful **human oversight** over the factual premises of administrative action. As analyzed in the Metodo Giuridico study on *Algorithmic Decisions between Automation and the Human Oversight Reserve*, compliance with the principle of legality and the rule against exclusively automated decision-making requires that computerized standardization of workflows always preserve substantive verification by natural-person officials — an indispensable safeguard to avert blind automatism and ensure an effective **human-in-the-loop reserve** within administrative proceedings[D4].

2.2 — Accredited Flaggers, the Asymmetric Evidentiary Regime, and the Duty of Utmost Diligence

The proper functioning of the enforcement mechanism designed by AGCOM rests upon a markedly asymmetric **allocation of the burden of proof**, crafted to balance urgent interim intervention against the reliability of underlying factual findings. Article 2(3) and (4) of Law no. 93/2023 confers standing to submit blocking requests upon rightholders, their licensees, collective management organizations, and entities accredited as **trusted flaggers**. Each submission must be supported by rigorous technical documentation attesting to the ongoing nature of the infringement and the actual unauthorized dissemination of protected works, uploaded under the reporting entity's **direct civil and criminal liability**.

Operational experience gathered during the platform's first two years of activity nevertheless exposed the risk of summary or technically flawed notices capable of affecting IP addresses not exclusively dedicated to unlawful streaming. To address that vulnerability, the Authority adopted **Resolution no. 209/25/CONS**, enacting a comprehensive overhaul of Article 10 of the Online Copyright Enforcement Regulation. The amended rules impose an express obligation upon accredited entities to act with the **utmost professional diligence** and rigorous technical verification, categorically prohibiting the reporting of network resources that carry a high risk of indiscriminate collateral blocking. Breaching this standard of care does not merely constitute a formal irregularity, but triggers the administrative sanction of **immediate suspension** or revocation of platform accreditation ordered by AGCOM.

The progressive layering of statutory and regulatory provisions has thus shaped a comprehensive legal regime, whose structural evolution across the sector's regulatory milestones may be summarized as follows:

Regulatory Dimension	Original Framework (Resolution no. 680/13/CONS)	Current Framework (Law no. 93/2023 & Resolution no. 209/25/CONS)
Legal Basis of Power	Secondary regulation grounded in general clauses of Law no. 249/1997 and Legislative Decree no. 70/2003.	Express primary statute under Article 2 of Law no. 93/2023 complemented by Article 9 of the Digital Services Act.
Blocking Timeframe	Ordinary proceedings within 35 days; expedited urgent procedure within 12 days.	Rapid disabling via Piracy Shield within thirty minutes of notification.
Addressees of Orders	*Mere conduit* access providers established and operating in Italy.	All intermediaries, including foreign DNS, VPN, and CDN providers as well as search engines.
Anti-Overblocking Safeguards	Ex ante case-by-case administrative investigation conducted by AGCOM offices.	Predominant unlawful use test, duty of utmost diligence, and six-month periodic unblocking review.

Proceduralizing the rightholders' duty of diligence transforms the technical report into a **legally qualified procedural act**. Rather than acting as a mere complainant, the accredited flagger assumes a **guarantor position** safeguarding the integrity of electronic communications networks. Attaching stringent disqualifying consequences to negligent or abusive data submissions supplies the necessary counterweight to the extraordinary speed of the blocking order, restoring equilibrium between **intellectual property enforcement** and the immunity of digital resources unrelated to unlawful conduct.

03. THE SUPRANATIONAL PERIMETER: PIRACY SHIELD BLOCKING ORDERS AND COMPATIBILITY WITH EUROPEAN UNION LAW

3.1 — From the Prohibition of General Monitoring to Outcome-Based Injunctions: Case Law of the Court of Justice

National instruments designed to combat online piracy must continually be measured against the system of fundamental safeguards and liability exemptions established by European Union law. Ever since the inception of EU electronic commerce regulation, now recodified in Article 8 of **Regulation (EU) 2022/2065**, a foundational rule has stipulated that *"No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers."* This **prohibition of general monitoring** seeks to preserve the **technological neutrality** of network operators, preventing intermediaries from being turned into private censorship bodies or burdened with disproportionate duties of preventive surveillance across all data streams carried over their infrastructure.

The case law of the **Court of Justice of the European Union (CJEU)** delineated the scope of that prohibition in its seminal judgment in *Scarlet Extended*, holding that EU law precludes any judicial or administrative order requiring an internet access provider to install a **generalized filtering system** operating permanently and exclusively at its own expense[3]. The Luxembourg Court explained that indiscriminate filtering of all electronic communications would infringe the intermediary's **freedom to conduct a business** guaranteed under Article 16 of the Charter of Fundamental Rights of the European Union, while simultaneously undermining end-users' rights to the protection of personal data and freedom to receive and impart information under Articles 8 and 11 of the Charter. Crucially, the ruling underscored the danger that insufficiently selective automated filters could unlawfully block legitimate communications, given that lawful use often depends on statutory exceptions and limitations that purely algorithmic tools cannot reliably assess.

Building on this line of European precedent, specialized legal scholarship has drawn a sharp distinction between impermissible preventive surveillance and **targeted injunctions** aimed at specific unlawful content[D5]. Indeed, the ban on general monitoring does not preclude competent national authorities from issuing specific orders requiring intermediaries to terminate or prevent concrete infringements, provided that the subject matter of the measure is unambiguously identified and does not compel the operator to conduct autonomous legal assessments regarding the lawfulness of transmitted streams. The constitutional equilibrium thus lies in shifting from proactive surveillance duties to executive obligations of **reactive technical cooperation**, under which the burden of identifying unlawful content remains squarely vested in rightholders and public authorities.

3.2 — The Doctrinal Evolution from Scarlet Extended to UPC Telekabel Wien and Glawischnig-Piesczek

The strict **prohibition against preventive general filtering** established in *Scarlet Extended* was subsequently refined and complemented by the Court of Justice of the European Union in *UPC Telekabel Wien*[4]. Asked to determine the compatibility with EU law of a court order directing an internet access provider to block user access to a copyright-infringing website without specifying the exact technical measures to be implemented, the Court upheld the full lawfulness of **outcome-based injunctions**. The European judges reasoned that such an approach leaves the addressee free to select the technical tools best suited to its operational resources and capabilities, enabling it to avoid coercive penalties by demonstrating that it has taken all reasonable steps to impede unauthorized access. Such an injunction fully satisfies the **fair balance of fundamental rights** mandated by Article 52(1) of the EU Charter, provided that the measures deployed do not unnecessarily deprive internet users of lawful access to available information and have the effect of seriously discouraging unauthorized viewing of protected works.

A further decisive **doctrinal milestone** in constructing the supranational framework emerged in *Glawischnig-Piesczek*, where the **Court of Justice of the European Union** addressed the recurring dissemination of unlawful material across digital platforms[5]. The Court ruled that the prohibition against general monitoring obligations does not preclude a judicial or administrative authority from ordering an intermediary to remove or disable access not only to information previously declared unlawful, but also to **identical or equivalent content** disseminated by the same user or by third parties. The lawfulness of extending the injunction rests on the indispensable condition that the specific elements of the infringement are precisely delineated in the original order and that minor formal variations do not require the intermediary to carry out an **independent legal assessment**, allowing the provider instead to rely on automated search and filtering technologies.

The judicial reasoning articulated in *Glawischnig-Piesczek* supplies the foundational logical and legal premise underpinning **dynamic injunctions**. Were a blocking order strictly confined to the exact character strings or numerical network identifiers verified at the outset of proceedings, infringers could effortlessly neutralize its prohibitive effect

through trivial domain-extension changes or by migrating the stream to an adjacent server. Recognizing the validity of orders extending to equivalent infringing feeds anchors the binding force of the administrative command to the substantive core of the infringement, preserving the **practical effectiveness** (*effet utile*) of legal remedies without turning the intermediary into an arbiter of online legality.

3.3 — Article 17 of the Copyright Directive, the Poland Judgment, and the Balancing of Fundamental Rights

The definitive synthesis between electronic commerce immunities and urgent enforcement of intellectual property rights crystallized in the scrutiny of **Directive (EU) 2019/790** — and specifically **Article 17** thereof — conducted by the **Court of Justice of the European Union** in *Republic of Poland v European Parliament and Council*[6]. In dismissing the action for annulment brought by the Member State against the liability regime applicable to online content-sharing service providers, the Grand Chamber mapped out the constitutional coordinates within which automated filtering and disabling technologies comply with Article 52 of the Charter of Fundamental Rights. The judgment emphasized that any limitation on the exercise of **freedom of expression and information** protected under Article 11 of the Charter must be provided for by law and respect the **principle of proportionality**, requiring clear statutory rules that strictly define the scope and conditions of public interference.

The defining feature of that ruling lies in its holding that algorithmic blocking mechanisms are compatible with the EU Treaties only when accompanied by robust **structural safeguards** protecting end-users and lawful content. Requiring intermediaries to make best efforts to prevent the availability of unauthorized works encounters an insurmountable limit in the mandatory preservation of legitimate uses, such as statutory exceptions for quotation, criticism, review, or parody. Accordingly, the Court held that legislation must enforce a **negative obligation of result**: automated filtering systems must not prevent the availability of content whose unlawfulness is not manifestly established. Furthermore, user protection requires mandatory, expeditious, and effective complaint and redress mechanisms whose final determinations are unfailingly subject to **human review** and effective **judicial scrutiny**.

The constitutional paradigm articulated by the Court in *Poland* projects its interpretive force directly onto the regulation of urgent dynamic blocking orders. Although Article 17 of the Copyright Directive specifically governs content-sharing platforms, the balancing standards developed therein permeate the entire body of European digital services law. Consequently, the operational speed achieved through algorithmic execution can never harden into an irrebuttable presumption that every flagged resource is unlawful. Rather, the legal order demands that the swiftness of the prohibitory command be matched by timely procedural remedies enabling operators of lawful services erroneously affected by a block to obtain prompt restoration of network routing, thereby preserving the delicate equilibrium between exclusive intellectual property rights and informational pluralism.

04. FOREIGN PROVIDERS OF DNS, VPN, AND CDN SERVICES BEFORE THE ITALIAN LEGAL ORDER: THE CLOUDFLARE LITIGATION

4.1 — The Doctrinal Distinction Between Articles 9 and 56 DSA and the Country-of-Origin Principle

The practical effectiveness of digital anti-piracy enforcement inevitably confronts the cross-border structure of global internet infrastructure. Because authoritative and recursive **DNS resolution services**, virtual private networks (VPNs), and content delivery networks (CDNs) are predominantly operated by multinational corporations established outside national territory, thorny disputes over jurisdiction and administrative competence have arisen. In the high-profile

litigation brought by **Cloudflare Inc.** challenging AGCOM's prohibitory and sanctioning resolutions, the **Regional Administrative Court (*TAR*) of Lazio** conducted a systematic doctrinal examination of the interplay between domestic regulatory sovereignty and EU digital services law[7]. The Rome administrative court rejected the US provider's contention that appointing a European legal representative in Portugal vested exclusive supervisory and enforcement jurisdiction in the Portuguese national authority pursuant to Article 56 of the Digital Services Act.

The judgment elucidated the clear functional divide separating **Articles 9 and 56 of Regulation (EU) 2022/2065**. Article 56 governs general supervision and enforcement of the systemic due-diligence obligations imposed directly by the Regulation upon intermediary providers, allocating exclusive competence to the **Digital Services Coordinator** of the Member State of main establishment. Conversely, Article 9 expressly recognizes the power of national judicial or administrative authorities to issue orders to act against specific items of illegal content, anchoring competence in the Member State where the infringing content produces its **harmful effects**. **Piracy Shield blocking orders** do not constitute structural supervisory measures regulating an intermediary's general terms of service; rather, they operate as targeted injunctions aimed at suppressing intellectual property infringements consummated within the Italian market, fully grounded in the territorial criterion of service destination.

> Member States' digital sovereignty does not yield before the global architecture of the internet: the harmful-effects principle legitimizes national blocking orders directed at any technical intermediary providing the channel through which an infringement propagates.

From this premise follows the inapplicability of the **country-of-origin principle** as a blanket immunity shielding cross-border conduct that inflicts localized harm on defined national markets. A foreign provider offering *reverse proxy* or public recursive DNS resolution accessible to users in Italy cannot invoke technical neutrality as a ground to disregard a lawfully issued domestic order. In extending disabling obligations to service providers wherever established or located, Article 2(3) of Law no. 93/2023 operates squarely within the **European Union safeguard clause**, ensuring that the geographic location of servers or corporate headquarters does not create an enforcement-free zone exempt from injunctions protecting exclusive copyright.

4.2 — TAR Lazio Judgment no. 13201/2026 and the Irrelevance of the Foreign Seat of the Legal Representative (TAR Lazio Judgment no. 13202/2026)

The complementarity of multilevel enforcement received full confirmation in the companion judgment handed down by the **Regional Administrative Court (*TAR*) of Lazio** in proceedings brought by Cloudflare Portugal Unipessoal Lda, the European legal representative designated by the US parent company pursuant to **Article 13 DSA**[8]. The administrative bench held that designating a legal representative within the Union serves a purely facilitative function for formal service of documents and institutional liaison with public authorities, without in any way transferring **exclusive injunctive jurisdiction** to the Member State in which that subsidiary entity is established. Holding otherwise would enable opportunistic regulatory *forum shopping*, allowing global digital corporations to neutralize administrative orders issued by national authorities simply by incorporating instrumental corporate vehicles in jurisdictions perceived as less stringent.

On strictly procedural grounds, Judgment no. 13202/2026 carries central importance because it clarifies the legal nature of individual **blocking tickets** transmitted through the automated platform. The court rejected the applicant's

argument that each technical ticket constitutes an autonomous administrative measure vitiated by inadequate investigation and breach of prior adversarial hearing rights. Dynamic injunctions do not create new legal obligations altering the intermediary's substantive sphere; instead, they operate as **executive acts** continuously updating the original framework prohibitory order so as to prevent circumvention of the primary command. Providing **deferred adversarial review** through the post-execution complaint mechanism fully satisfies the **procedural defense guarantees** enshrined in Article 24 of the Italian Constitution and Article 6 of the European Convention on Human Rights.

Legal scholarship commenting on the twin judgments of the Regional Administrative Court (*TAR*) of Lazio has underscored how affirming domestic jurisdiction over public DNS resolvers and cross-border VPN operators marks a decisive advance in upholding legality online, subjecting actors that had hitherto operated at the periphery of national regulation to binding duties of administrative and judicial cooperation[D6]. Extraterritorial enforcement thus converges with the **principle of proximate harm**: any provider operating network services that optimize and route traffic toward a domestic audience cannot evade the determinations of the competent national regulator and must deploy appropriate technical measures — including **geo-targeted blocking** — to halt the dissemination of infringing streams within the boundaries of state jurisdiction.

05. AGCOM'S SANCTIONING POWER AND FINE CALCULATION BASED ON WORLDWIDE TURNOVER

5.1 — The Primary Statutory Basis of Pecuniary Sanctions and Article 1(31) of Law no. 249/1997

The deterrent credibility of any regulatory regime presupposes a **statutorily defined and proportionate sanctioning framework** capable of discouraging opportunistic or dilatory conduct by market actors. As noted in the historical reconstruction above, the chief vulnerability undermining Italy's pre-2023 anti-piracy system lay in the absence of primary legislation attaching pecuniary penalties to non-compliance with AGCOM's blocking orders. That structural gap was closed by **Article 5 of Law no. 93/2023**, which expressly provides that whenever addressees fail to execute urgent interim orders or associated dynamic injunctions, AGCOM shall impose the pecuniary administrative sanctions set forth under **Article 1(31) of Law no. 249 of 31 July 1997**.

Under that statutory provision, non-compliance with orders issued by the Authority triggers a **pecuniary penalty** ranging between two and five per cent of the turnover achieved by the undertaking during the last financial year closed prior to notification of the statement of objections. Conducting sanctioning proceedings requires strict adherence to the general guarantees codified in **Law no. 689/1981** governing statutory legality, culpability, personal liability, and timely service of formal charges. In cross-border cases where the addressee resides outside Italian territory, the mandatory ninety-day statutory time-bar (*decadenza*) applicable to domestic entities is replaced by the broader **three-hundred-and-sixty-day time limit** laid down in Article 14(2) of Law no. 689/1981, ensuring effective and timely state enforcement even vis-à-vis overseas technology conglomerates.

Administrative case law has likewise confirmed the full compatibility of AGCOM's sanctioning procedure with the fair-trial standards guaranteed by Article 6 ECHR, emphasizing that the functional separation between investigative offices and the collegiate decision-making board safeguards **procedural participation rights**. An intermediary charged with non-compliance enjoys the right to inspect the administrative file, submit written defense briefs, and request an oral hearing; moreover, subjecting the final penalty resolution to **full judicial review on both law and merits** (*giurisdizione di merito*) before the Regional Administrative Court (*TAR*) ensures that any procedural defect or excessive quantification can be corrected by an independent court, preserving constitutional defense rights throughout every stage of proceedings.

5.2 — Quantification of the Fine in Resolution no. 333/25/CONS and Proportionality Criteria

Practical enforcement of this statutory sanctioning power reached its landmark test with the adoption of **Resolution no. 333/25/CONS**, whereby AGCOM issued an administrative penalty order imposing a fine of EUR 14,247,698.56 on **Cloudflare Inc.** for persistent refusal to comply with the blocking order issued in **Resolution no. 49/25/CONS**. Challenging the financial assessment of the fine, the company alleged manifest disproportionality and sharply criticized the Authority's decision to calculate the statutory percentage not against revenues generated within Italy, but against the corporate group's **consolidated worldwide turnover** exceeding USD 1.6 billion.

The **Regional Administrative Court (*TAR*) of Lazio** upheld AGCOM's methodology in full, grounding its ruling in both the unambiguous wording of the primary statute and compelling law-and-economics reasoning. **Article 1(31) of Law no. 249/1997** refers generally to the undertaking's turnover without introducing any geographic or territorial restriction — a limitation that would have required an express statutory carve-out. Furthermore, because the foreign parent corporation supplies and monetizes its network services directly from abroad without maintaining a permanent commercial establishment in Italy, pegging the fine solely to revenues formally booked in Italy would have yielded negligible penalties, frustrating the **deterrent function of administrative sanctions** and creating an arbitrary competitive distortion to the detriment of domestic operators whose entire turnover is billed domestically.

The operational interplay between national sanctioning powers and the European architecture of the Digital Services Act may be systematically contrasted in the following comparative table:

EU Legal Parameter	Article 9 Regulation (EU) 2022/2065	Article 56 Regulation (EU) 2022/2065
Subject Matter of Measure	Specific order to act against identified items of illegal content accessible within national territory.	General supervision over compliance with systemic terms-of-service and due-diligence obligations.
Competent Authority	Judicial or administrative authority of the affected Member State (AGCOM for Italy).	Digital Services Coordinator of the Member State of main establishment (or the European Commission).
Role of EU Legal Representative	Irrelevant to substantive injunctive competence; serves solely as legal contact point for notifications.	Anchors exclusive territorial competence for supervising systemic obligations of non-EU providers.
Associated Sanctioning Power	National pecuniary penalty assessed against consolidated worldwide turnover for non-compliance.	EU-level fines of up to six per cent of annual worldwide turnover for breaches of the DSA.

This interpretive stance adopted by the Regional Administrative Court (*TAR*) of Lazio aligns Italian electronic communications law with contemporary European digital enforcement regimes, under which the **economic capacity of the infringing undertaking** is consistently measured by reference to consolidated global financial statements. Calibrating pecuniary sanctions to the true operational scale of a multinational enterprise restores the effectiveness of domestic public law, preventing corporate fragmentation or the absence of local subsidiaries from conferring *de facto* financial immunity upon major internet intermediaries.

06. UNRESOLVED CRITICAL ISSUES: OVERBLOCKING, DEFERRED ADVERSARIAL REVIEW, AND ACCESS TO TECHNICAL RECORDS

6.1 — Shared IP Addresses, the Amendments of Law no. 143/2024, and Resolution no. 209/25/CONS

Notwithstanding its consistent endorsement by administrative courts, the practical operation of Italy's anti-piracy mechanism continues to raise complex technical and legal tensions concerning collateral impacts on innocent third parties. The foremost vulnerability stems from the contemporary **architecture of internet routing protocols**, in which widespread reliance on shared *cloud hosting* and CDN distribution means that a single numerical IP address may simultaneously host hundreds of entirely lawful websites and digital applications alongside a single unauthorized stream. Under such conditions, indiscriminate execution of **Piracy Shield blocking orders** at the IP routing layer risks triggering **collateral overblocking** — namely, the unjustified disruption of legitimate business operations and lawful digital services.

To contain such spillover effects, Parliament intervened through **Law no. 143 of 9 October 2024** (converting Law Decree no. 113/2024 into law), enacting targeted amendments to Article 2 of Law no. 93/2023. The statutory threshold governing IP-level blocking was reformulated by replacing the earlier requirement of resources uniquely dedicated to infringement with the standard of IP addresses *"predominantly dedicated"* to unlawful activities. While facilitating enforcement against mixed-use hosting environments, this statutory shift heightens the analytical burden and legal responsibility borne by accredited flaggers, requiring rigorous quantitative verification that unlawful streaming accounts for the preponderant share of traffic hosted on the targeted address. The 2024 reform also inserted paragraph 5-bis, mandating **periodic six-month unblocking reviews** of network identifiers no longer used for unlawful purposes, and introduced **Article 174-sexies** into the Italian Copyright Law, imposing an express statutory duty upon intermediary providers to report criminal piracy offenses to judicial authorities.

This set of statutory corrective measures was operationalized by AGCOM through **Resolution no. 209/25/CONS**, bringing sector regulations into alignment with the amended legislative text. Annex A to that Resolution codified an express prohibition barring rightholders from submitting blocking requests targeting network resources that pose a high risk of **collateral overblocking**, conditioning platform access upon strict compliance audits. Technical prudence is further reinforced by AGCOM's power to rely on operational cooperation from the Financial Guard (*Guardia di Finanza*) and the Postal and Communications Police to verify the accuracy of submitted data, establishing a multi-layered web of safeguards aimed at preventing urgent enforcement from impairing the **operational continuity** of lawful third-party digital services.

6.2 — The Ten-Day Administrative Complaint Procedure and Limits on Document Access under TAR Lazio Judgment no. 14414/2024

Reconciling immediate executive enforcement with the procedural rights of affected parties ultimately hinges upon **deferred adversarial review** exercised through the **administrative complaint procedure**. Under the initial regulatory text, addressees of a blocking order were granted a narrow window of just five days to challenge the measure before AGCOM. Through the amendments enacted by **Resolution no. 209/25/CONS** (Annex A, Article 10(7)), that time limit was appropriately doubled to ten days from the disabling of access. Standing to lodge a complaint was likewise expressly extended to any third party demonstrating a **qualified legitimate interest** (*interesse qualificato*), exercisable within ten days of gaining actual knowledge of the documented absence of statutory prerequisites. Filing a complaint initiates full adversarial review before AGCOM's collegiate board, ensuring prompt revocation of the block whenever an erroneous flag is established.

Effective exercise of defense remedies nonetheless presupposes access to the technical records underlying a blocking measure — an issue on which the **Regional Administrative Court (*TAR*) of Lazio** has taken a markedly restrictive stance[9]. Ruling on a special judicial access action brought under Article 116 of the Code of Administrative Judicial Procedure by an industry association seeking bulk disclosure of all tickets, domain names, and IP addresses blocked through Piracy Shield during its initial months of operation, the court dismissed the application in its entirety. The bench held that standing for **defensive access to administrative documents** cannot be presumed in the abstract from trade representation or participation in technical roundtables, but must be specifically proven in relation to a concrete, direct, and individualized legal interest. A blanket request aimed at auditing the entirety of blocking measures issued by the platform runs afoul of the statutory **prohibition against generalized oversight** of administrative action codified in Article 24(3) of Law no. 241 of 7 August 1990.

Disputes over disclosure of source code, computer logs, and platform algorithms intersect broader administrative law doctrines governing technical trade secrets and algorithmic transparency. As examined in the Metodo Giuridico study on *Defensive Access and Technical Secrets under the New Public Contracts Code*, administrative courts have carefully delineated the balance between the right of judicial defense and protection of **industrial and technological confidentiality** covering proprietary software systems, making clear that document access can never degenerate into an exploratory fishing expedition[D7]. Within the Piracy Shield ecosystem, preserving the confidentiality of algorithmic specifications also serves imperative **cybersecurity** needs by preventing criminal piracy networks from reverse-engineering technical filters. What emerges is a calibrated informational asymmetry: while an affected addressee or injured third party may obtain targeted access solely to records concerning its specific network resource, the systemic architecture of the platform remains shielded under AGCOM's institutional oversight.

07. SYSTEMATIC SYNTHESIS AND FUTURE PROSPECTS OF ADMINISTRATIVE ANTI-PIRACY ENFORCEMENT

The foregoing investigation enables a coherent doctrinal synthesis of the Italian anti-piracy enforcement regime shaped by **Law no. 93/2023** and its implementing regulations. The overall resilience displayed by this framework when tested before the administrative courts attests to a successful transition from a fragmented regulatory model lacking primary statutory penalties to a structured public-law system capable of combining rapid interim intervention with the core constitutional guarantees of **administrative due process** and statutory legality. Qualifying **Piracy Shield blocking orders** as **progressively structured outcome-based injunctions** has withstood challenges grounded in the judicial

reserve and proportionality principles, positioning administrative enforcement in constructive complementarity with ordinary civil and criminal remedies.

At the European Union level, the analysis has demonstrated that effective protection of intellectual property rights requires a rigorous, non-evasive reading of the **Digital Services Act**. The functional allocation of competences between Articles 9 and 56 of Regulation (EU) 2022/2065 preserves **Member States' regulatory sovereignty** in repressing unlawful conduct producing harmful effects within their territories, preventing corporate establishment abroad or the appointment of a legal representative in another Member State from serving as a shield of immunity for cross-border technical intermediaries. Assessing pecuniary administrative fines against the intermediary's **consolidated worldwide turnover**, far from constituting a disproportionate punitive anomaly, gives concrete effect to the economic principle of **effective deterrence**, averting competitive distortions against domestic providers and ensuring that global infrastructure platforms actively contribute to legality across the digital ecosystem.

Looking ahead, the evolution of this enforcement model nonetheless demands sustained vigilance over the points of friction revealed by operational practice. Refining technical standards for identifying predominantly infringing IP addresses and strengthening accredited flaggers' duties of diligence under **Resolution no. 209/25/CONS** chart the proper course toward minimizing systemic collateral overblocking across shared cloud infrastructure. At the same time, extending the complaint deadline to ten days and maintaining rigorous judicial review before the administrative courts provide vital institutional safeguards against investigative overreach, ensuring that the extraordinary speed of procedural automation never erodes the core guarantees of defense rights and **substantive adversarial review**.

References & Authorities Cited

Statutory Provisions

- Law no. 93 of 14 July 2023 — Provisions for the prevention and repression of the unlawful dissemination of copyright-protected content across electronic communications networks.
- Law no. 143 of 9 October 2024 — Conversion into law of Law Decree no. 113 of 9 August 2024 laying down urgent tax measures and extensions of statutory deadlines (Omnibus Decree).
- Law no. 249 of 31 July 1997 — Establishment of the Italian Communications Authority (AGCOM) and rules governing telecommunications and broadcasting systems (in particular Article 1(31)).
- Law no. 633 of 22 April 1941 — Protection of copyright and related rights (Italian Copyright Law, in particular Articles 156 and 174-sexies).
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 — Single Market For Digital Services (Digital Services Act, in particular Articles 8, 9, 13, and 56).
- AGCOM Resolution no. 189/23/CONS of 26 July 2023 — Amendments to the Regulation on online copyright enforcement across electronic communications networks.

- AGCOM Resolution no. 321/23/CONS of 5 December 2023 — Completion of the acquisition and operational deployment of the unified technological platform named Piracy Shield.

- AGCOM Resolution no. 49/25/CONS of 18 February 2025 — Prohibitory order requiring disabling of DNS resolution and network traffic routing issued against Cloudflare Inc.

- AGCOM Resolution no. 209/25/CONS of 30 July 2025 — Amendments to the Regulation on online copyright protection across electronic networks and revised Article 10 governing live events.

- AGCOM Resolution no. 333/25/CONS of 29 December 2025 — Pecuniary penalty order imposing an administrative fine of EUR 14,247,698.56 on Cloudflare Inc. for non-compliance with blocking orders.

Case Law Cited

1. **Council of State (*Consiglio di Stato*), Judgment of 15 July 2019, no. 4993** — Confirms the full lawfulness of AGCOM's regulatory competence and urgent administrative injunctive powers to protect online copyright, while precluding the introduction of pecuniary administrative sanctions via secondary regulation absent an express primary statutory basis. Outcome: upheld in part (annulling regulatory pecuniary penalties) and dismissed as to the remainder. Para.: §§ 16, 17, and 20.

2. **Regional Administrative Court (*TAR*) of Lazio, Judgment of 22 January 2024, no. 1223** — Recognizes the proportionality of the thirty-minute maximum time limit for disabling access to unauthorized live streams and confirms the full compatibility of the dual-track system combining AGCOM administrative enforcement with ordinary civil jurisdiction. Outcome: dismissed (application and additional grounds). Para.: §§ 1.1 and 1.2.

3. **Court of Justice of the European Union (CJEU), Judgment of 24 November 2011, Case C-70/10, no. 771/2011, *Scarlet Extended*** — Holds that an injunction requiring an internet intermediary to install a generalized, permanent preventive filtering system infringes the freedom to conduct a business, personal data protection, and users' freedom of information. Outcome: upheld opposition to injunction (declaring generalized preventive filtering precluded by EU law). Para.: §§ 48, 50, and 52.

4. **Court of Justice of the European Union (CJEU), Judgment of 27 March 2014, Case C-314/12, no. 192/2014, *UPC Telekabel Wien*** — Permits outcome-based injunctions requiring an intermediary to block access to infringing websites while leaving the choice of concrete technical measures to the addressee, provided users are not unnecessarily deprived of lawful access to information. Outcome: upheld compatibility of targeted outcome-based injunctions. Para.: §§ 52, 62, and 63.

5. **Court of Justice of the European Union (CJEU), Judgment of 3 October 2019, Case C-18/18, no. 821/2019, *Glawischnig-Piesczek*** — Confirms the lawfulness of injunctions extending removal or disabling obligations to identical or equivalent information, provided specific identifying elements are defined in the order so that the intermediary is not required to carry out an independent legal assessment. Outcome: upheld admissibility of injunctions covering identical or equivalent content. Para.: §§ 41, 45, and 46.

6. **Court of Justice of the European Union (CJEU), Judgment of 26 April 2022, Case C-401/19, no. 297/2022, *Republic of Poland v European Parliament and Council*** — Declares automated content-blocking mechanisms compatible with the EU Charter of Fundamental Rights solely when accompanied by strict safeguards protecting lawful uses, the prohibition of general monitoring, and complaint procedures subject to human review. Outcome: dismissed action for annulment against Article 17 of Directive (EU) 2019/790. Para.: §§ 67, 85, and 90.

7. **Regional Administrative Court (*TAR*) of Lazio, Judgment of 17 July 2026, no. 13201** — Affirms AGCOM's domestic competence to issue blocking orders against foreign technical providers under Article 9 DSA, qualifies dynamic tickets as executive acts implementing the framework order, and upholds fine calculation against consolidated worldwide turnover. Outcome: declared joined applications partly inadmissible, partly time-barred, and dismissed on the merits as to the remainder. Para.: §§ 6.5, 16.2, and 19.4.

8. **Regional Administrative Court (*TAR*) of Lazio, Judgment of 17 July 2026, no. 13202** — Rules out that designating a European legal representative in Portugal under Article 13 DSA transfers injunctive competence over infringements producing domestic harmful effects, confirming the executive nature of dynamic blocking tickets. Outcome: declared joined applications partly inadmissible, partly time-barred, and dismissed on the merits as to the remainder. Para.: §§ 3.1 and 3.2.

9. **Regional Administrative Court (*TAR*) of Lazio, Judgment of 15 July 2024, no. 14414** — Denies bulk disclosure of domain names and IP addresses blocked through the Piracy Shield platform for lack of proven individualized standing and pursuant to the bar on generalized oversight of administrative action under Article 24(3) of Law no. 241/1990. Outcome: dismissed application for defensive document access. Para.: concluding grounds.

Legal Scholarship Cited

D1. **Bruno Tassone**, *Primo commento alla legge sulla pirateria online e al regolamento AGCOM* [First Commentary on the Online Piracy Law and the AGCOM Regulation], in *Il Diritto Industriale*, no. 5/2023, p. 415 ff. — Preliminary analysis of the statutory innovations introduced by Law no. 93/2023 and the urgent interim powers conferred upon the Communications Authority.

D2. **Marcello Stella**, *Access provider e tutela inibitoria* [Access Providers and Injunctive Relief], in *Rivista di Diritto Processuale*, no. 3/2023, p. 891 ff. — Doctrinal study on the legal nature of dynamic injunctions directed at third-party intermediaries and the structuring of procedural adversarial guarantees.

D3. **Diego Cacciatore**, *Diffusione illecita di contenuti sportivi e responsabilità degli Internet Service Provider* [Unlawful Dissemination of Sports Content and Liability of Internet Service Providers], in *Il Diritto Industriale*, no. 6/2025, p. 562 ff. — Examination of live sports audiovisual protection and the technical impact of the thirty-minute blocking window on network operators.

D4. Metodo Giuridico, *Decisioni algoritmiche tra automazione e riserva di umanità* [Algorithmic Decisions between Automation and the Human Oversight Reserve]. Systematic analysis of the non-exclusivity principle in algorithmic decision-making and the preservation of human oversight in administrative proceedings.

D5. **Francesca Santoro**, *Novità sulla disabilitazione dell'accesso a contenuti diffusi online abusivamente* [Developments on Disabling Access to Content Unlawfully Disseminated Online], in *Il Quotidiano Giuridico*, 22 October 2024 — Commentary on the procedural innovations of Law no. 93/2023 and the operational criteria governing rapid blocking orders.

D6. **Giuseppe Cassano**, *Piracy Shield e blocchi transfrontalieri verso i fornitori esteri di DNS e VPN* [Piracy Shield and Cross-Border Blocking Against Foreign DNS and VPN Providers], in *Il Quotidiano Giuridico*, 28 August 2026 — Analysis of the extraterritorial reach of AGCOM blocking orders vis-à-vis multinational technology platforms in light of the TAR Lazio rulings.

D7. Metodo Giuridico, *Accesso difensivo e segreti tecnici nel nuovo Codice appalti* [Defensive Access and Technical Secrets under the New Public Contracts Code]. Reconstruction of the balancing test between judicial defense needs and industrial confidentiality over source code and algorithms.

GM

Giovanni Ercole Moscarini

AUTHOR • METODO GIURIDICO

Attorney at the Rome Bar

Practises civil law and administrative law. For Metodo Giuridico he analyses statutory developments and judicial trends across both fields.