AUDIOVISUAL ANTI-PIRACY ALLIANCE

Live broadcast piracy in Europe: the case for a three-layered regulatory response

Position paper · October 2026

1. Executive summary

Live broadcast piracy in Europe is growing, not receding. In November 2025 the Commission's own assessment of Recommendation (EU) 2023/1018 found that it has not delivered the improvement it sought.[1] The sector has exhausted what voluntary engagement can achieve; legislation is now required. AAPA's May 2026 submission to the Call for Evidence on the review of EU copyright rules set out the ecosystem, the critical role of hosting providers and European ICT, and the regulatory gaps.[2] This paper updates that position in light of the Commission's consultation, and proposes three measures as a single layered solution:

- **Layer A — Notice and takedown that works at live speed.** A binding obligation on hosting providers to remove live pirated content as near to immediately as is reasonably and/or technically achievable and, in any event, within 30 minutes of a valid notice, with meaningful stay-down measures, effective supervision and deterrent sanctions for systematic non-compliance.
- **Layer B — A consequence for those who will not comply.** A competent authority designates the networks of hosting providers that persistently fail to act on notices and whose networks are predominantly used for piracy and other illegal content. The designation is entered in a live Union-wide register and, on publication, triggers binding obligations on providers established in, or offering services in, the Union not to serve the designated operator in respect of those resources or carry traffic to them.
- **Layer C — A dynamic live blocking backstop in every Member State.** Every Member State must provide a mechanism for live content that meets common minimum principles and a binding capability test at Union level. Whatever institutional route a Member State chooses, the mechanism must be capable of adding and updating verified targets within the live window, without a fresh application for each event or target, while preserving effective review and redress.

> **The three measures are cumulative, not alternatives. Lack of timely takedown needs a consequence; the consequence needs a defined standard of non-compliance to attach to; both need a backstop. Adopt one without the others and the problem stays where it is.**

2. Why legislative action is now necessary

Live piracy can no longer be treated as an intellectual property problem alone. The networks carrying a stolen broadcast into a European home are the same ones carrying malware, fraud and unverified television into it, and artificial intelligence is accelerating all of it. It is now a cybersecurity and consumer protection problem too, and that is what has strengthened the case for legislating.

The scale is no longer marginal. The EUIPO's own survey of European citizens found that 14% had intentionally used illegal sources for online content in the past year, 12% specifically to watch sport, and 11% had used an illicit streaming device or application; among 15–24 year-olds each figure roughly doubles, to 33%, 27% and 25% respectively.[3] AAPA's economic research estimates that 31.2 million Europeans used illicit IPTV in 2025, at a cost of €4.32 billion to the legitimate industry. User numbers are up 82.5% since

[1] Commission Staff Working Document, *Assessment of Commission Recommendation (EU) 2023/1018 on combating online piracy of sports and other live events*, SWD(2025) 384 final, 20 November 2025.

[2] AAPA, *Live Piracy Ecosystem, critical role of hosting providers and European ICT, and the key regulatory gaps requiring immediate action by European lawmakers*, May 2026, submitted to the Commission's Call for Evidence on the review of EU copyright rules.

[3] EUIPO / European Commission, *European Citizens and Intellectual Property* (2023) — self-reported, and therefore more likely to understate than overstate. On the exposure of younger audiences to illicit gambling, pornography and financial scams, AAPA, *Live Piracy Ecosystem* (2026), pp. 2–3.

2021, and visits to live sport piracy sites per internet user climbed roughly a third between late 2023 and early 2025 — that is, after the Recommendation had taken effect.[4]

Crime and cyberthreats are now intertwined with piracy

The pirated stream is not only the product but the lure. AAPA research found that 57% of pirate IPTV applications tested carried malware, and that more than half of that malware enrols the subscriber's own broadband connection into residential proxy pools — so the household's line is used to disguise other people's fraud, eroding the IP-reputation defences banks, retailers and public services rely on.[5] The intertwining is structural, not incidental: on several of the hosting networks serving live piracy, audiovisual infringement is not even the largest category of illegal activity, sitting beneath phishing, malware and botnet control on the same networks and the same operators (section 3). Action against the hosts that carry live piracy is therefore action against serious cybercrime.

Pirate IPTV also delivers unregulated, unverified television into millions of European homes: thousands of live channels, with no oversight under the Audiovisual Media Services Directive, no national regulator and no verification of a channel's origin. The Union has already decided that some of this content must not reach European homes — the Council has suspended the broadcasting activities of several Russian State-controlled outlets, and the prohibition expressly extends to distribution by IPTV — yet member monitoring finds those same channels still listed in the packages illicit IPTV services sell to European consumers.[6] What piracy defeats here is therefore not only copyright but a restrictive measure the Union has already taken, and the same unsupervised route is open to anyone else seeking that reach into European homes. This also raises concerns for the protection of minors. Illicit IPTV packages can place adult and other harmful content alongside ordinary entertainment, without reliable age restrictions or parental safeguards. Parents cannot assume that the protections they expect from regulated audiovisual services apply, leaving children potentially exposed to content unsuitable for their age.

Artificial intelligence is turbocharging the whole ecosystem

Pirate operators now market AI-optimised infrastructure and automated multi-language support as selling points, and AI is compressing the cycle by which pirates register and rotate domains, network numbers and hosting, with full redeployment observed within minutes of a takedown. Nor is AI only an accelerant: it is already being turned against the protections the broadcasting sector relies on, including techniques that break the pairing between a stream and the forensic marking used to trace it, and further problems specific to live broadcasting should be expected.[7] This ecosystem is now rebuilt faster than it can be dismantled, and the time available to act is shrinking.

The remedy the sector relies on cannot answer any of it

Notice and takedown, the sector's only practical real-time remedy, is failing. Grant Thornton's analysis of the notice data rights owners submitted to the EUIPO found that only 11% of notices resulted in a stream being suspended, 66% were ignored entirely, 90% of illegal streams reappeared within 24 hours, and only 6% received any reply within 30 minutes. Under the same duty, online platforms suspend infringing content during the event in around 96% of cases, while hosting providers manage fewer than 10%.[8] The standard is plainly achievable; what is missing is the obligation. The reason is structural: a live broadcast's commercial value is consumed while it is being transmitted, so a takedown the next morning is a takedown

[4]AAPA, *Economic Impact of Illicit IPTV in Europe and North Africa*, interim report, 15 May 2026, which also estimates unrealised VAT and corporate tax revenue across the 37 countries surveyed at approximately €1.08 billion a year.

[5]AAPA, *Illicit IPTV in Europe* (2022) for the malware finding; Enders Analysis (2025) for the residential proxy finding.

[6]Directive 2010/13/EU (Audiovisual Media Services Directive), as amended; Council Decisions suspending the broadcasting activities of certain Russian State-controlled outlets, the prohibition in which expressly extends to distribution by IPTV. The continued carriage is AAPA member monitoring of illicit IPTV services' own published channel guides — industry monitoring, not a regulator finding.

[7]AAPA member monitoring and open-source reporting (2026). No EU study yet consolidates AI's role in piracy specifically, and that absence is itself part of the argument; the interference with forensic marking is member operational experience rather than published research.

[8]Grant Thornton, analysis for the Live Content Coalition of the rights-owner takedown notice data submitted to the EUIPO (2025). The comparison of platform and hosting-provider suspension rates is drawn from the notice data reported under the EUIPO's monitoring of Recommendation (EU) 2023/1018.

of nothing. European law has never defined "expeditious" in that context, and in its absence a diligent hosting provider carries a cost its non-compliant competitor does not.[9]

Nor is the live broadcasting sector asking the European Union to solve a problem it has not tried to solve itself. Major broadcasters deploy industry-leading protection — forensic watermarking, the highest content protection standards, real-time detection — but no network of that complexity can be defended against every attack, and a single stolen stream can then be replicated infinitely: an echo chamber in which one breach feeds the entire ecosystem. Criminal prosecution does put pirate operations out of business, but those cases take years. Nor can regulation reach the pirates directly: proxy registrations, shell companies, layered resellers and crypto payments mean a rights owner frequently cannot establish who operates a service, from where, or against whom proceedings could be brought.

3. Where regulation can reach: the facilitators

Pirates do, however, depend on identifiable, established businesses to reach a European viewer — most European, most already subject to European law: hosting providers and online platforms, which store and serve the stream; transit and peering providers, which carry it across the internet, on which non-compliant hosts most depend, and which have rarely, if ever, been made subject to piracy-related obligations; residential ISPs, the last hop into the home; the search, social, messaging and marketplace services promoting piracy; and data centres, CDNs, reverse proxies, domain registrars and DNS services. None operates anonymously; all are licensed or contractually reachable undertakings that can be placed under enforceable obligations.

Of these, hosting is the closest point to the source that regulation can realistically reach. A pirate cannot put a stream on the internet without a hosting provider: it stores the stream, serves it and gives it passage across the network. Acting there removes what everything downstream would otherwise carry — fewer blocking orders, a lighter burden on the platforms promoting piracy.

The large, established hosting providers substantially comply with the notices rights owners send, and many act within minutes. They are not the problem. The problem is that, on the AAPA members' own monitoring, as much as 85% of the hosting landscape now serving live piracy comprises offshore, non-compliant providers, such as shell entities in low-disclosure jurisdictions, with no verifiable identity, no premises, no staff and no meaningful abuse function, which do not respond to notices and in many cases advertise that they will not.

They can operate because the resources they need ask little of them — network numbers, IP ranges, domain names, server capacity and transit are obtainable with minimal verifiable identity, and published abuse contacts are frequently false or defunct. In the case of domain names, that is so despite an existing Union requirement: Article 28 of Directive (EU) 2022/2555 (NIS2) obliges registries and registrars to maintain accurate and complete registration data, to verify it, and to provide it to legitimate access seekers without undue delay. That obligation should be enforced effectively: false registration data relied on by a pirate service should carry consequences, and rights owners and competent authorities should be able to obtain accurate registration data promptly for live enforcement.

An AAPA / Xploratio study of ten of these networks, selected from members' reports, found no case in which piracy was incidental: on three, audiovisual piracy accounted for three quarters or more of all content observed; on one, it was about a tenth, with phishing, spam, malware and other malicious infrastructure about half; on another it sat beneath unlicensed gambling. None was a general-purpose host — which can be verified by a competent authority before designating anything.

Two facts make a European remedy possible. Their corporate identity is offshore, which defeats legal process; but in the study of ten such providers, more than 90% of the server infrastructure identified for them sits, according to commercial geolocation services, inside the European Union, and they depend on European transit and interconnection to reach European consumers.[10] Both are deliberate choices, and the

[9] Regulation (EU) 2022/2065 (Digital Services Act): the notice-and-action mechanism is Article 16, while the requirement to act "expeditiously" sits in the hosting exemption in Article 6, successor to Article 14 of Directive 2000/31/EC.

[10] The 85% figure is the aggregate of AAPA members' operational monitoring of the live piracy hosting landscape and is offered as an estimate, not a published study. The >90% figure and the traffic composition are from AAPA / Xploratio, *Offshore Non-Compliant Audiovisual Piracy Hosting Providers* (2026), a study co-authored by AAPA of ten providers selected because members had reported them: shares of the domain names and addresses flagged within the part of each provider's address space that was scanned, categories as reported, and not every category reported for every provider. Server locations are as reported by commercial IP geolocation services.

second is the opportunity: the remedy must be directed at the infrastructure rather than at the shell company.

4. The three-layered solution

Layer A — notice and takedown that works at live speed

What our members propose is that the obligation on a hosting provider making live content available be codified in the following terms:

> **Takedown:** *"As near to immediate as is reasonably and/or technically achievable, and commensurate with the live nature of the content being infringed, and in any event no more than 30 minutes from receipt of the notice."*
>
> **Stay-down:** *"Upon receipt of a notice from a rights owner, the hosting provider must also take meaningful and effective measures to mitigate further infringement of the live content, including effective action against repeat infringing customers and technical measures directed at the notified content."*

The formulation is a deliberate double lock: near-immediate action is the standard, with 30 minutes as the outer limit, so it cannot be read as a licence to take 29 minutes where a provider could act in two. That limit is not arbitrary — it has been accepted as the applicable standard by a national court, and compliant providers routinely act well inside it. The legal framework should permit effective supervision, accreditation of trusted reporting systems and deterrent sanctions for repeated failure to meet the live standard. Stay-down is only enforceable if the provider knows who its customer is; hosting providers and the undertakings supplying network numbers, IP addresses, domain names, server capacity and transit should therefore identify and verify their business customers and beneficial owners and, for domain names, consistently with the verification duties already imposed on registrars by Article 28 of NIS2.

This is not a new burden: compliant providers already meet it, running 24/7 abuse and trust-and-safety functions, much of it automated. Codification levels the playing field and creates the legal test everything else depends on: without a defined deadline, non-compliance cannot be established and Layer B (see below) has nothing to attach to. A provider unable to meet the standard should not be hosting live streamed content.

Alongside the hosting obligation, the framework should also provide for actionable notices to other intermediaries materially involved in facilitating the infringement, including data centres, CDNs and reverse proxies, transit providers, domain registrars, DNS services and relevant online platforms. Each should take measures appropriate to its role and technical capability to stop the notified infringement during the live broadcast and mitigate its recurrence. These obligations should distinguish removal at source, withdrawal of supporting services, disabling access and removal of promotional listings. This complements, and does not replace, Layers B and C.

Layer B — a consequence for the deliberately non-compliant

Tighter takedown obligations alone will drive piracy further towards providers who have no intention of complying. We therefore propose a designation mechanism in four steps:

1. Rights owners, or accredited monitoring bodies acting for them, report through the competent authority's administrative platform the Autonomous System Numbers (ASNs) of hosting providers that persistently fail to comply, with the supporting evidence. An ASN is a network's unique, published identifier in the internet's own routing registries — how other providers already know whose traffic they carry.
2. A competent authority designates, on the basis of published criteria. Two conditions must always be met: a substantial and persistent volume of notices has gone unanswered, and the network is predominantly used to make available illegal content, as defined in the Digital Services Act, assessed together with any other illegal use that can be positively identified. In addition, the operator must have placed itself beyond effective reach: either it offers services in the Union without a legal representative under the Digital Services Act or has failed to act on an order under it, or its registration or abuse-contact data is false, invalid or unresponsive. The procedure must be capable of urgent designation without prior warning where advance notice would defeat the measure. Designation without prior warning must be followed by rapid review and effective judicial redress.

3. The designation is published immediately in a maintained, public and machine-readable Union-wide register of designated ASNs. As the ordinary effect of a Regulation, publication should trigger legal effect across the Union without parallel proceedings in each Member State. The operator and any affected third party must have access to rapid review and appeal, and designations must be reviewed periodically and lifted when the grounds no longer apply, including where the provider becomes compliant. Designating at network level against a live register, rather than against a corporate name, is what prevents evasion by re-registration.
4. Providers established in, or offering services in, the Union are placed under a legal obligation not to serve the designated operator in respect of designated ASNs, and not to carry traffic to those networks, without undue delay and in any event within 24 hours of publication. The obligation does not extend to internet access services provided to end users, which are the subject of Layer C.

Apart from the duties described under Layer A, only the fourth step places a new obligation on anyone, and it requires no fundamentally new network capability. European ICT providers already deploy route filtering, IP prefix blocking and null routing, de-peering, contract termination and traffic scrubbing against botnets, command-and-control servers, malware, phishing infrastructure, sanctions evasion and sanctioned entities. It has been done in practice, for example in 2018 a European hosting operator was cut off by six connectivity providers and dropped by three major internet exchanges on the evidence alone, without legislation, though a fourth kept carrying it. In 2025, the Council itself designated a hosting provider under Regulation (EU) 2024/2642 for supplying infrastructure to state-sponsored actors, although the operation reorganised around the listing, which is why designation must attach to network resources rather than to a company. The tooling, the practice and the legal template all exist. What is missing is a piracy-specific designation process and a binding duty to act on it. Requiring upstream providers to take proportionate measures against piracy facilitated by identified non-compliant hosts is consistent with the risk-based approach already adopted across NIS2, the Cyber Resilience Act, the Digital Services Act and the AI Act.

Layer C — a dynamic live blocking backstop in every Member State

Every Member State should be required to provide a dynamic blocking mechanism for live content that is proportionate and effective — an obligation of result, not of means — with minimum principles harmonised at Union level. Member States should remain free to use the judicial, administrative or combined route that fits their constitutional order. In every case, however, the mechanism must pass the same capability test: once the legal basis and methodology have been approved, verified targets must be capable of being added and updated during the live window without a fresh application for each event or technical target. Those principles should require that any mechanism is:

- transparent, and clearly governed by law;
- proportionate, with safeguards against over-blocking, clear rules on which services a measure may reach, rapid correction of errors and effective independent oversight and judicial redress;
- genuinely dynamic — updatable during a live broadcast through an automated end-to-end process under supervision, with accredited rights owners or their agents able to submit verified targets directly once the methodology has been approved, subject to audit, traceability and accountability;
- broadly available — against any intermediary materially able to help stop or frustrate the infringement, including ISPs, DNS providers, VPN services, search engines, registrars, proxy services and other relevant technical intermediaries; and
- enforceable, with compliance monitoring, information-gathering powers, corrective orders and deterrent sanctions, including stronger consequences for repeated or systematic non-compliance, and accessible to rights owners at proportionate cost.

Several Member States have already legislated for this, and their experience answers the feasibility question. In France, Article L.333-10 of the Sports Code supports blocking for a whole season, updated as pirate services move and administered by Arcom; the measures now reach search engines, DNS resolvers, registrars and VPN providers as well as ISPs. In Italy, Law 93/2023 requires blocking within 30 minutes through an automated platform operated by AGCOM. Together, these frameworks show that a genuinely dynamic remedy and a 30-minute standard are achievable at scale. A harmonised Union framework should combine their strengths: a legal measure lasting for a duration which is the most effective at disrupting

piracy in practice, with new technical targets added dynamically and without a fresh application. Targets should remain blocked while the criteria continue to be met, subject to periodic re-verification and rapid correction of error or lawful reassignment.

Registrars should be treated in the same way as the other intermediaries within the scope of these measures: orders reaching them must be equally dynamic, so that they extend to replacement domain names registered by the same operator without a fresh application.

5. Safeguards and proportionality

These proposals are directed at infrastructure shown, on evidence and by a competent authority, to exist for illicit purposes. They do not ask intermediaries to police content or accept liability for it. Designation under Layer B would rest on published criteria, be open to review and appeal and be reversible on compliance; blocking under Layer C would be governed by law, supervised and constrained against over-blocking. Any such measures must comply with the principles established by the Court of Justice — proportionality, effective judicial protection, specificity of targeting and the protection of fundamental rights under Article 52 of the Charter — and in AAPA's view they do.

Measures against registrars fit within those principles: they act on a specific, identified domain name, are reversible, and require no monitoring of content.

6. The alternative, and the case for acting on all three

If these measures are not adopted, lawmakers will be driven to expand the scope of the Digital Services Act — the promotion and discovery services pirates rely on already fall within it, but compliance falls short and its scope is too narrow to dent piracy — a far broader and more intrusive instrument than anything proposed here.

Acting at the source will make Europeans safer by denying cybercriminals infrastructure and audiences sustained by piracy. AAPA urges binding Union action across all three layers, requiring effective outcomes and live capability while respecting national constitutional arrangements and judicial review.