# THE BENEFITS AND COSTS OF WEBSITE-BLOCKING LEGISLATION: AN ECONOMIC, LEGAL AND POLICY ASSESSMENT

J. Scott Marcus, Artur Bogucki and Jacob Griffith

**CEPS IN-DEPTH ANALYSIS**

April, 2026-03

# SUMMARY

This study seeks to provide an independent, evidence-based assessment of the economic costs and benefits of Member State website-blocking laws and practices in the EU-27. The study is inspired by a number of recent Member State measures that, in attempting to curb online piracy, require the blocking of web content in burdensome ways while arguably failing to fully achieve the stated objective of tackling intellectual property violations.

Our analysis suggests that website blocking is associated with substantial risk of unintended consequences and harmful side effects, which may not be fully appreciated by the Member State authorities either enacting relevant regulation or issuing blocking orders. Rightsholders tend to be quick to call for blocking solutions, because they bear none of the costs, which fall instead to providers of intermediary services and internet users more broadly.

Piracy is a complex phenomenon that cannot be solved solely by technical measures like blocking. Solid academic literature tells us that legal and illegal consumption are substitutes for one another. Blocking merely seeks to increase the cost of illegal consumption. A better strategy would place at least as much emphasis on increasing content availability and convenience, on reducing fragmentation and delay, and on cutting the price of legal consumption, thereby enhancing the desirability of legal consumption.

J. Scott Marcus is an Associate Senior Research Fellow in the Global Governance, Regulation, Innovation and Digital Economy (GRID) unti at CEPS. Artur Bogucki is an Associate Researcher in the GRID unit at CEPS. Jacob Griffith is a Research Assistant in the GRID unit at CEPS.



CEPS • Place du Congrès 1 • B-1000 Brussels • Tel: (32.2) 229.39.11

# CONTENTS

# FIGURES & TABLE

# EXECUTIVE SUMMARY

In recent years, we have witnessed a proliferation of new EU Member State measures and cases that seek to block the access of the public to specific internet content. These have been enacted at the Member State level, mainly in an effort to reduce online piracy. But little consideration has been given to their apparently limited effectiveness, or of the possible risk of overblocking, much less the costs imposed on network operators and service providers. The enactment of different and mutually inconsistent rules by different Member States has led to fragmentation and tension between these rules and EU guarantees of freedom of expression (as embodied for instance in the goals of the Open Internet Regulation).

This study seeks to provide an independent, evidence-based assessment of the economic costs and benefits of Member State website blocking laws and practices in the EU-27. It is inspired by recent Member State measures and case law that, in attempting to curb online piracy, require the blocking of web content in burdensome ways, while possibly missing the goal of preventing intellectual property violations.

## BACKGROUND

There are legitimate reasons to block internet content. Some content may be illegal. Some may be a manifestation of hybrid warfare. Yet most of the noteworthy blocking in recent years has been motivated by the desire to reduce copyright infringement of audiovisual content, i.e. pirated streaming.

The most common technologies used today are (i) IP address blocking, (ii) Domain Name System (DNS)-resolver blocking, and (iii) Deep Packet Inspection blocking. Blocking approaches are also distinguished by the time frames in which they operate. Blocking can be static, dynamic, or live (i.e. near real-time). For each technology and for each modality of blocking, there are many ways to circumvent it.

Many EU Member States (and the UK) have implemented blocking arrangements. They differ from one another in numerous dimensions, including initial controls on blocking, rights of appeal, and the time frame in which blocking is implemented. These divergent rules pose a challenge for cross-border operations.

In the jurisprudence of Court of Justice of the European Union, a key consideration for the permissibility of blocking obligations is the principle of proportionality.

Still, given the economic incentives to view pirated content and that the technical means to do so (despite any website blocking) are readily available, plus the ease with which

blocking can be circumvented, it is unlikely that piracy can be fully contained solely by means of blocking.

### ATTITUDES AND PRACTICES OF EU CONSUMERS REGARDING COPYRIGHTED ONLINE CONTENT

Many experts would argue that overall copyright policy has totally run off the rails. Copyright was initially envisaged as a limited-time arrangement, with costs that need to be balanced against its negative impact on many forms of innovation.

The European public could be said to recognise this tension. They acknowledge the overall value of the copyright regime at a philosophical, if not at a practical or personal level. In a survey of more than 25 000 EU individuals conducted by the EU Intellectual Property Office (EUIPO) in 2023, 93% see value in copyright protection; however, 44% overall feel that strict protection of intellectual property curbs innovation, including 57% in the 15–24 age group. Less than 10% of those surveyed felt that intellectual property enforcement benefits SMEs, or consumers like themselves.

In some (eastern) EU Member States, a majority feel that it is acceptable to obtain online content illegally when it is for personal use. Meanwhile, 48% of EU respondents aged 15–24 find it acceptable to access content illegally if it is only for personal use, compared with 27% of those aged 55–64 or 28% of those aged 65 and over.

Some 14% of Europeans overall (or about one in 7) admit to having intentionally used illegal sources to access content online, while 33% of Europeans in the 15–24 age group admit to having done so. Even so, this may be under-reported – some respondents may have been reluctant to 'out' themselves.

Price and availability appear to play a huge role in the willingness to access content illegally. Notably, 43% of those who use online content from illegal sources report that lower prices might lead them to stop doing so; conversely, 44% report that the main reason they do not access content illegally is because the content they want is available via legal sources.

For illegal on-demand non-IPTV consumption of films, average consumption appears to have declined from 2.6 visits per internet user per month in January 2017 to 0.9 visits per month at the end of 2023, the latest available date for the data.

For both films and music, there is a wealth of solid, peer-reviewed research that supports the claim that the decline in illegal consumption can be attributed to increasing availability and decreasing prices over time. When content is available legally, on a timely basis and at a reasonable price, piracy drops; conversely, lack of availability, delays (e.g.

due to release windows), fragmentation among different content platforms, over-pricing, or inconvenience tend to drive a rise in piracy.

The use of website blocking to prevent copyright infringement of audiovisual sports content in particular implies both some of the greatest economic rewards and also some of the greatest risks of website overblocking.

### HARMFUL SIDE EFFECTS

The practical effects of website blocking tend to be limited and short-lived. Users are good at bypassing blockages, and pirate websites are good at migrating to unblocked venues.

As a result, past academic literature tends to suggest that website blocking generates only limited positive effects, and that blocking is effective only when imposed on many websites at once, and in conjunction with expanding the availability and lowering the cost of legal alternatives.

More recently, Danaher et al. (2023) found no consistent evidence of displacement of users from blocked illegal websites to unblocked illegal websites, but they found a fairly small but statistically significant overall increase in consumption of legal content of 8.1%, 3.1%, and 5.2% in the two blocking waves in India and one in Brazil, respectively. There are, however, no reliable estimates of the longevity of the effects of website blocking.

The burden of website blocking typically falls on parties other than those responsible for the infringement – chiefly on network operators, on providers of independent DNS resolution services, on providers of content delivery networks, or very recently on providers of VPNs. This creates challenges for global operators that (unlike ISPs, which operate within a defined national territory) run distributed infrastructure spanning many countries simultaneously, with no native mechanism for restricting a measure to users in a single jurisdiction.

Website blocking regimes across the EU to date have consistently proven to be flawed and overly broad, owing to a combination of institutional shortcomings, technical limitations inherent to the blocking methods employed, and misaligned incentive structures. The rightsholder does not bear the cost of the blockage.

Even if near-real-time blockage makes a modest contribution to enforcement, it precludes proper procedural safeguards to ensure that blockage is not overinclusive, and does not inappropriately impact freedom of expression.

The laws in question here are being implemented at Member State level, but no two are alike. This is damaging to the EU single market. The risk that this fragmentation might

pose undue burdens on cross-border operations has perhaps been underestimated by Member State authorities, who do not themselves bear the costs, and also by EU policymakers, for whom the issue is not yet very visible.

### OTHER TOOLS ARE NEGLECTED

We would argue that the approach at EU and Member State levels, and by the rightsholders themselves, has focused excessively on one set of enforcement tools, without paying sufficient attention to other approaches that are probably more effective in the longer term, and with fewer negative side effects. Policy to date has concentrated on limiting access to the *supply* of infringing content, without paying sufficient attention to the *demand* for infringing content, mainly because the current approach is painless for the rightsholders.

A study by the EUIPO has stated this clearly. 'Enforcement is challenging due to technological sophistication, jurisdictional issues and consumer demand for cheap content. … [*A*] *multifaceted approach involving technology, legal efforts, and education is essential to combat this issue effectively*' (emphasis added) (Bornas Cayuela, Djail, & Wajsman, 2024, p. 10).

Many important tools are in the hands of the rightsholders themselves. EUIPO survey data indicate that 43% of those who use online content from illegal sources report that lower prices might lead them to stop doing so; conversely, 44% report that the main reason they do not access content illegally is because the content they want is available via legal sources.

Availability and convenience are also crucial contributors to piracy, arguably even more so than price. Transmissions of sports, other events, and films are typically limited to a single country or a single language group by *geo-blocking* – a practice that would be viewed as being anti-competitive were it not for the intersection with copyright law. And broadcast rights for sports are often fragmented across multiple transmission platforms such that a viewer who wants to closely follow a single sports team may be forced to either subscribe to multiple platforms at a combined price that is prohibitive, or else resort to infringement. An owner of a Spanish LaLiga 2 club recently posted a complaint that he cannot follow his own team's matches without multiple paid subscriptions, and that even so, he often finds it impossible to watch his own team's games when he is outside Spain (Voulgaris, 2026).

The European Commission has argued along the same lines. Paragraph 33 of their Recommendation on combating online piracy of sports and other live events (European Commission, 2023) states: 'Holders of rights in live transmissions of sports and other

events should be encouraged to increase the availability, affordability, and attractiveness of their commercial offers to end users across the Union.'

EUIPO survey data suggest that 90% of users are aware of legal offers; still, a large fraction of users is sometimes uncertain as to whether the offer that they are accessing is in fact legal. Raising user awareness therefore also has a role to play.

In terms of remedying problems of illegal content, there is an opportunity to better focus enforcement where it is likely to be most effective and least harmful. Where feasible, this would be the entity that hosts the data; otherwise, the point closest to the user. The philosophy of Recitals 27 through 29 of the Digital Services Act should play as large a role as possible. We think that they should be understood as relevant to infringing content as well. Recital 27 specifically explains that responsibility for dealing with illegal content cannot fall solely to providers of intermediary services. The sense of these recitals is that illegal or infringing content (under the laws of the country of use) should be acted on at the level with greatest specificity, and thus least likely to cause collateral damage.

In line with Recital 27, one might suppose that it would be ideal to remove content altogether where it is hosted, but there are legal and practical constraints on what can be done. Some content will be hosted in a different country from that where it is used. The content might be permissible in the country of origin, but illegal in the country of use. Providers of pirated content will naturally prefer to host content in countries that are lax in enforcing intellectual property rights. It is the country of use that has unambiguous ability to enforce its rules, including rules regarding copyright. In any event, blocking infringing content at or near the source might or might not be effective – it might simply motivate pirates to move the point at which infringement takes place.

Beyond these more fundamental changes, many procedural improvements are possible in the blocking process itself.

### RECOMMENDATIONS

Our analysis suggests that website blocking is associated with substantial risk of harmful side effects, which may not be fully appreciated by the Member State authorities issuing the blocking orders. Rightsholders will tend to be quick to call for blocking solutions, because they bear none of the costs, which fall instead to providers of intermediary services.

More generally, rightsholders are motivated to block as much as possible in order to enhance their profitability. It is up to policymakers to strike the right balance, ensuring that EU fundamental freedoms, including freedom of expression, are protected at the same time.

Piracy cannot be solved by blocking alone. Solid academic literature tells us that legal and illegal consumption are substitutes for one another. Blocking seeks solely to raise the cost of illegal consumption. A better strategy would place at least as much emphasis on increasing availability and convenience, on reducing fragmentation and delay, and on cutting the price of legal consumption, thereby increasing the desirability of legal consumption.

A brief recap of our recommendations follows. Substantiation for the rationale for each appears in Chapter 5 of the main report.

### *Recommendations to rightsholders*

- Rightsholders would be well advised to reflect on their pricing schemes and on any restrictions on availability and convenience (including fragmentation across multiple platforms, together with geo-blocking) that they impose. The most effective means of combating piracy would be to ensure widespread availability of affordable content. The gains in reduced piracy should be evaluated together with gains from an increase in consumption in light of the high elasticity of consumer demand for content.
- Whenever legally and practically feasible, rightsholders should first pursue infringers who reproduce their content without consent before addressing intermediaries.

### *Recommendations to the European Union*

- Measures to assist users in distinguishing legal from illegal content, including improved education, should be part of any comprehensive strategy to combat online piracy.
- Whether content is illegal or infringing needs to be judged for the purpose of blocking under the laws of the country of use, not those of the country of origin.
- Additional guidance at EU level on whether to block, and if so, then how, is called for, taking into account the principle of subsidiarity, the need to avoid fragmentation of the EU single market, and the growing need to avoid unnecessary burden on the sector (including on intermediaries that have little or nothing to do with any infringing content).
- IP-based blocking should be avoided altogether. To the extent that blocking is used at all, better targeted mechanisms such as DNS-level or URL-level blocking should be used instead.

- Reforms should be considered to better align incentives. Rightsholders should be required to contribute to the costs of implementing blocking measures, proportionate to the scale and complexity of the blocking requested, and they should bear liability for damages caused by overblocking implemented at their request.
- Enforcement and coordination of the blocking of hybrid warfare content should be strengthened, and national regulators should be provided with sufficient technical capacity and clear guidance to ensure consistent implementation across the EU-27.

### *Recommendations to the Member States*

- Blocking orders should be subject to prior or rapid judicial review.
- Blocking orders should be time-limited with periodic review, and the geographical scope should be clearly defined and limited as much as possible.
- Any delegation of blocking authority to private entities must be accompanied by meaningful oversight and safeguards.
- As part of their proportionality assessment, national regulators should assess blocking orders for compliance with Article 3(3) of the Open Internet Regulation before implementation, not merely after the fact.

# 1. INTRODUCTION

To curb online piracy, various recent Member State measures and case law may require the blocking of web content in burdensome ways, while possibly missing the objective to reduce intellectual property violations. This study, conducted by CEPS at the request of Nord Security and with their support, assesses trends in website blocking, identifies costs and benefits, and suggests possible ways forward.

## 1.1 OBJECTIVES

In the last few years, we have witnessed a number of new EU Member State measures and cases that seek to block the access of the public to specific internet content. These have been enacted at Member State level, mainly in an effort to reduce online piracy. But there has been little consideration of their apparently limited effectiveness, the possible risk of overblocking, or the costs imposed on network operators and service providers. The enactment of different and mutually inconsistent rules by different Member States has led to fragmentation and tension between these rules and EU guarantees of freedom of expression. The latter are embodied for instance in the goals of the Open Internet Regulation ((EU) 2015/2120), which seeks to ensure that network operators 'treat all traffic equally … without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided'.

This study seeks to provide an independent, evidence-based assessment of the economic costs and benefits of Member State website blocking laws and practices in the EU-27. We have reviewed recent measures, evaluated the costs and burdens associated with them, and how the costs are distributed along the value chain. We have also collected available information on the degree to which these measures are, or are not, likely to be effective and fit for purpose in achieving their stated objectives. Furthermore, we summarise the literature on the prevalence and underlying drivers of piracy of copyrighted content.

The concern of rightsholders over piracy is understandable. Data from the EU Intellectual Property Office (EUIPO) (Bornas Cayuela, Djail, & Wajsman, 2024) suggests that the average rate of piracy is more than 10 accesses per internet user per month, suggesting a substantial loss of potential revenue for rightsholders. We caution, however, that this average probably lumps together some users who very often view pirated content with others who rarely if ever do so.

The technology to circumvent website blocking (including for example encrypted Domain Name System (DNS) technologies such as DNS-over-HTTPS (DoH) / DNS-over-TLS (DoT) is readily available and steadily improving. At the same time, there appear to be many

reasons for consumers to want to circumvent restrictions, including the bypassing of geo-blocking and over-pricing relative to consumer willingness to pay for highly desired content such as sports, together with a fragmented EU market for audiovisual content. Under these circumstances, containing piracy can be expected to be challenging, irrespective of the means used to do so. A growing body of literature suggests that technical measures are effective only briefly before consumers figure out how to successfully get around them.

## 1.2 METHODOLOGY

Our study is based on a mix of desk research and literature review, coupled with comparative analysis.

Our desk research and literature review seek to map EU legislative initiatives and their justifications (including copyright law, the Digital Services Act (DSA) (Regulation (EU) 2022/2065) and net neutrality under the Open Internet Regulation). It identifies significant examples from the EU-27 and selected case studies of Member State implementation, such as content blocking following geopolitical crises (e.g. linked to Russia's aggression against Ukraine). For case studies, especially as regards alleged copyright infringement, we benefit from a recent paper by Analysys Mason (Abecassis, Daly, & Glickman, 2025) on behalf of Cloudflare. Data on piracy is subject to obvious limitations, but we have based our research primarily on the biennial reports of the EUIPO (Bornas Cayuela, Djail, & Wajsman, 2024).

We use this evidence base to provide comparative analysis contrasting the projected benefits of website blocking measures with their economic and social costs. This draws on legal analysis, existing Commission impact assessments and support studies, general studies on the economic effects of copyright and net neutrality (including our own), and available data. We evaluate both direct and indirect costs, such as innovation losses, reduced competitiveness, impediments to freedom of expression, and user harm.

## 1.3 STRUCTURE OF THIS REPORT

Following this Introduction, we present the general background in Chapter 2. We then discuss the benefits of website blocking in Chapter 3, and the costs of website blocking in Chapter 4. We then conclude with recommendations in Chapter 5.

Consistent with our usual practice, we make recommendations at the point in the text at which they are substantiated, and then collect a numbered list of recommendations at the end of Chapter 5 of this report, together with the number of the page on which the recommendation is substantiated.

# 2. BACKGROUND

**Key findings**

- There are legitimate reasons to block internet content. Some content may be illegal. Some may be a manifestation of hybrid warfare.
- Yet most of the blocking in recent years has been motivated by the desire to reduce copyright infringement of audiovisual content, i.e. pirated streaming.
- The most common technologies used today are (i) IP address blocking, (ii) DNS-resolver blocking, and (iii) Deep Packet Inspection (DPI) blocking.
- Blocking approaches are also distinguished by the time frames in which they operate. Blocking can be static, dynamic, or live (i.e. near real-time).
- For each technology and for each modality of blocking, there are many limitations, and many ways to circumvent.
- Various EU Member States (and the UK) have implemented blocking arrangements. They differ from one another in many dimensions, including initial controls on blocking, rights of appeal, and the time frame for which blocking is applied.
- These divergent rules pose a challenge for cross-border operations.
- In the jurisprudence of the Court of Justice of the European Union (CJEU), a key consideration for the permissibility of blocking obligations is the principle of proportionality.
- Given the economic incentives to view pirated content and that the technical means to do so (despite any website blocking) are readily available, plus the ease with which blocking can be circumvented, it is unlikely that piracy can be fully contained solely by means of technical measures such as blocking.

In this chapter, we discuss the many different reasons to block website content (Section 2.1), the different ways in which content blocking is implemented, and the limitations associated with each (Section 2.2). We then discuss at length the situation under EU law and court rulings (Section 2.3), and the many measures that attempt to implement website blocking at Member State level (Section 2.4). We close with brief reflections on the implications for the EU single market (Section 2.5).

## 2.1 REASONS TO BLOCK

The hope of reducing online piracy is the most prominent driver of website blocking today, but by no means the only one.

Removing or disabling access to illegal content is another driver. The rationale and the mechanisms for doing so are spelled out in the DSA.

Yet another rationale is the blocking of state-sponsored content as a manifestation of hybrid warfare. This is the reason why content from Russian broadcasters was blocked shortly after Russia's barbaric invasion of Ukraine. In that case, however, the Council Recommendation provided no guidance as to what to block or how, leading to massive confusion on the part of network operators, and possibly infringing in part the network neutrality provisions of the Open Internet Regulation.

Still, most noteworthy blocking in recent years has been motivated by the desire to reduce copyright infringement of audiovisual content, i.e. pirated streaming (see Section 3.2).

## 2.2 IMPLEMENTATION OF CONTENT BLOCKING

In this section, we consider the different forms and modalities of content blocking restrictions, the limitations associated with various forms of content blocking, and the ease with which content blocking can be circumvented.

### *2.2.1 Different forms and modalities of content blocking*

Content blocking is implemented today using a range of different techniques and technologies, over different time scales, and with requests issued to different players. Each has its own strengths and weaknesses, as we explain in Section 2.2.2. None is perfect.

First, as far as technology is concerned, the taxonomy that appears in a study by Analysys Mason (Abecassis, Daly, & Glickman, 2025) on behalf of Cloudflare provides a good starting point. They identify three main technical approaches to website blocking: IP address blocking, DNS-resolver blocking, and DPI blocking. Each of these has limitations, as we explain in Section 2.2.3 and elsewhere.

- IP address blocking prevents traffic from being sent to or returned from IP addresses associated with restricted content. A block list is created containing individual IP addresses, or ranges of IP addresses, to be blocked.
- DNS-resolver blocking instead blocks the mapping of a domain name associated with restricted content to the corresponding IP address. A DNS resolver is a

specialised server that translates a URL provided by a user into the IP address needed to return the desired content to the user. But if the query sent to the DNS resolver from the end-user client device contains a domain specified in a block list, the DNS resolver will not return the requested IP address. Instead, it might return (i) a message indicating that the domain does not exist; (ii) an empty reply, causing the request to fail outright; or (iii) an IP address of a page of some different content (DNS poisoning), which can be a page explaining that access has been blocked, or an unrelated page that is not subject to access restrictions.

- DPI blocking entails inspecting the contents of individual data packets for potential threats from specific content, patterns or application types, in real time, as they pass an inspection point. DPI involves a high level of scrutiny of packets being conveyed over the internet.

Second, content blocking can be applied using different time frames or modalities: either in a static manner, in a dynamic manner, or in a live or near-real-time manner.

As blocking has spread across Member States, courts and rightsholders have adopted three increasingly sophisticated variants of blocking orders, each raising distinct proportionality concerns.

- Static blocking refers to a fixed list of domain names or IP addresses to be blocked, specified in a court order. The list does not change unless the court issues a new order. Static blocking orders were historically the norm.

- Dynamic blocking permits the rightsholder, usually without returning to court, to unilaterally add new domains or IP addresses to a blocking list. The initial court order establishes the blocking mechanism and its general parameters, but the rightsholder is then delegated authority to expand the list. Dynamic blocking is common in EU litigation, particularly in sports piracy cases. The EUIPO's 2021 study and its published guidance on dynamic blocking injunctions document the spread of this model.

- Live blocking is the most recent innovation. During broadcast events, particularly live sports matches, the rightsholder's technical team notifies ISPs of new pirated streams in real time, and ISPs are required to block them within minutes (for instance, 30 minutes in the Italian Piracy Shield model).

Third and last, blocking requests can be issued to market players at different levels of the value chain, including market players with little or no relationship to the restricted content, which is somewhat at variance from earlier practice.

### *2.2.2 Restrictions and limitations associated with various forms of content blocking*

Each of the techniques and modalities used for content blocking has its limitations.

IP address blocking is a simple technique, but with high probability leads to overblocking because a single IP address is likely to serve multiple users today. Innocent users are likely to be blocked along with the allegedly infringing user.

As a conspicuous example, the sharing of IP addresses across large numbers of unrelated customers is common for shared hosting providers, and is the core mechanism by means of which content delivery networks (CDNs) achieve scale.

Furthermore, the mapping between a domain and an IP address is neither fixed nor stable – CDNs rotate addresses dynamically, often using anycast routing (a technique where the same IP address is simultaneously announced from multiple geographical locations, routing different users to different physical servers). In consequence, a given IP address may serve entirely different content within minutes of a blocking order being made, while the targeted domain has already migrated elsewhere. This once again implies the risk that innocent users are impacted.

Under DNS-resolver blocking, a DNS resolver responds that the destination domain does not exist, or responds with the address of a different service that ideally explains somehow that access is blocked; but in many cases, this simply causes the request to malfunction. In practice, DNS-resolver blocking often leads to ambiguous or misleading behaviour vis-à-vis the end user. It will also often be the case that a single domain serves multiple users, thus raising the risk that innocent users are impacted together with infringing users.

The growing use of DoH and DoT cripples DNS-resolver blocking. Traditionally, when a user visited a website, their browser asked a DNS resolver to translate the domain name into an IP address. These queries were unencrypted, allowing ISPs or regulators to intercept them and block requests to certain domains. DoH and DoT now encrypt DNS lookups inside HTTPS/TLS connections, and this technology is easily accessible to users with only a few setting changes, including in popular browsers such as Chrome, Edge, and Firefox. The ICANN Security and Stability Advisory Committee's report, *DNS Blocking Revisited* (ICANN, 2025) confirms that encrypted DNS effectively neutralises traditional blocking, and that reimposing filtering would require decrypting user traffic, which violates privacy law and technical best practice.

Blocking by means of DPI provides much more granular control; however, it is computationally intensive, potentially invasive of privacy, and ineffective where content has been encrypted.

Static blocking offers the advantage of clear notice and periodic judicial review. Even so, static lists are quickly outdated as pirate operators migrate to new domains or IP addresses, which is why they have become largely superseded by more dynamic approaches. Static blocking also risks causing harm if the IP addresses in question (or the firm that holds them) is subsequently sold.

While dynamic blocking is more effective than static at combating piracy in real time, it raises heightened proportionality concerns: if the rightsholder has unilateral authority to request the blocking of new domains, the scope of the order can drift far beyond what the court originally envisaged, and the court does not perform *ex post* review of each new addition to the list.

Live blocking maximises piracy prevention but minimises proportionality: there is no opportunity for prior judicial review of the specific blocking instances, and the risk of errors is magnified. This is the model that has triggered the most aggressive regulatory backlash and the most documented collateral damage, as the national case studies below illustrate.

### *2.2.3 The ease of circumvention*

At the current level of technology, there are many ways to circumvent website blocking.

For IP address blocking, the simplest and most obvious circumvention is that the pirate site can simply move to a different domain name or a different IP address. This can potentially lead to a cat-and-mouse game where one domain is blocked, but pirated content rapidly reappears – often hosted in a country with lax enforcement of intellectual property rights.

This is already the case. Several studies find that the effects of website blocking have been short-lived in practice (see Section 4.1). A growing body of literature suggests that technical measures are effective only briefly before consumers figure out how to successfully circumvent them. This suggests that the effectiveness for general enforcement of copyright is limited.

Sports poses a special case. Sports content is very highly valued, both by consumers and in terms of payments from transmission media to rightsholders. Moreover, the value of sports content (as with news) declines very rapidly with time. For these reasons, even a block that is only briefly effective might play an important role in enforcing the

intellectual property rights; conversely, delay in imposing restrictions could mean that the restrictions are irrelevant.

For technological circumventions of website blocking technology, there is no shortage of means available. Notably, DNS-based blocking is among the most easily circumvented measures since a user need only change their configured DNS resolver to one that does not apply the block. Thousands of public and private DNS-resolver services are operated globally, some in jurisdictions with limited enforcement obligations if any, and a user can switch to a different DNS resolver in a matter of seconds through a single device setting. Beyond commercial alternatives, technically capable users can operate their own recursive DNS resolver, querying the global DNS root directly and bypassing any third-party filtering entirely. Additionally, the modern technology to circumvent website blocking (including for example encrypted DNS technologies such as DoH and DoT) is readily available and steadily improving.

At the same time, there appear to be many reasons for consumers to want to circumvent restrictions, including the bypassing of geo-blocking and over-pricing relative to consumer willingness to pay for highly desired content such as sports, together with a fragmented EU market for audiovisual content. In Section 3.2.2, we discuss survey results that indicate that many EU consumers tend to view illegal consumption of copyrighted content to be appropriate if the content is not available at a reasonable price.

Given that both economic incentives to view pirated content and the technical means to do so (despite any website blocking) are readily available, it is unlikely that piracy can be fully contained by means of blocking alone. Blocking seeks solely to limit access to the supply side aspects of piracy, i.e. to make pirated content less available. More promising would be to complement these measures with other tools that simultaneously seek to depress the demand side, i.e. to reduce consumer demand for pirated content.

## 2.3 COPYRIGHT: LEGAL COMPLEXITY AT EU LEVEL

In this section, we consider the legal basis for online copyright enforcement in general, key aspects of the case law at CJEU level, the interactions with the network neutrality portions of the Open Internet Regulation and the DSA.

### *2.3.1 The legal basis: InfoSoc Directive, Article 8(3) and Enforcement Directive, Article 11*

Website blocking enforcement in the EU rests on a two-pillar legal foundation established by the InfoSoc Directive 2001/29/EC and the Enforcement Directive 2004/48/EC. Article 8(3) of the InfoSoc Directive provides that Member States may enable rightsholders to seek an injunction against an intermediary whose services are used by a third party to

infringe intellectual property rights. This provision, paired with Article 11 of the Enforcement Directive, gives courts the power to order intermediaries to prevent or terminate intellectual property infringements.

The twin legal bases are intentionally broad, but the critical limitation is embedded in the text of Article 8(3): it stipulates that conditions and modalities relating to such injunctions should be left to the national law of the Member States. This delegation of implementation to the national level has produced the regulatory fragmentation observed today across the EU-27 (see also Section 2.4).

The implications were already apparent in the EUIPO's comprehensive 2021 study of blocking injunctions across the EU-27 (EUIPO, 2021). The study found that implementation is not uniform among the Member States, with critical differences in scope, procedure, oversight mechanisms, and available remedies. A *Stockholm IP Law Review* analysis noted that these differences mean that the effectiveness of blocking injunctions varies widely, creating legal uncertainty for both rightsholders and service providers operating across borders (Hagg, 2021). A CEPS 2015 special report (Renda, et al., 2015) that analysed the first decade of the InfoSoc Directive's implementation concluded that the objective of reducing fragmentation in the copyright regimes of the Member States had not been fully achieved (Ferri, 2021), a conclusion that remains apt a decade later (Zornetta, 2024).

### *2.3.2 The CJEU proportionality framework*

Although the InfoSoc Directive leaves implementation to the Member States, the CJEU has been active in setting outer boundaries through the principle of proportionality. The seminal cases establish a ladder of permissibility that national courts must navigate when issuing or reviewing website blocking orders.

- *Scarlet Extended* (C-70/10, 2011): general filtering prohibited. In its 2011 ruling, the CJEU held that a Member State cannot require an ISP to install and maintain a general, indiscriminate system for filtering and monitoring content transmitted over its network. Such a system would violate Article 15(1) of the E-Commerce Directive and Article 8(3) of the InfoSoc Directive by imposing an unjustified general monitoring obligation. Article 8 of the DSA carries this principle forward. The principle is clear: blanket surveillance is a breach of fundamental rights.
- *UPC Telekabel Wien* (C-314/12, 2014): targeted blocking with conditions permitted. Three years later, the CJEU tempered the absolutism of *Scarlet Extended*. A targeted blocking order against a specific pirate website can be compatible with EU law if it satisfies a proportionality test. The ISP must be free to choose the technical means, but any restriction on the freedom to conduct

business must strike a fair balance between the rights of the intellectual property holder, the freedom of information of internet users, and the legitimate interest of the ISP in optimising its network. Priority should therefore be given to prosecuting the operators of the illegal website and those who have contractual relations with them. The Court did not mandate a particular blocking technique; this discretion remains with the implementing authority.

- *Stichting Brein* v *Ziggo* (C-610/15, 2017): platform liability. The CJEU clarified that if a platform itself facilitates infringement, not merely as a neutral conduit but as an active intermediary that knowingly profits from piracy, it can be made subject to a blocking injunction. Even so, proportionality remains the key test. A broad, untargeted blocking order would fail the proportionality assessment, whereas a narrowly tailored injunction addressing specific infringing content hosted or streamed by that platform could be justified.

- *McFadden* (C-484/14, 2016): proportionate preventive measures. The CJEU held that a Member State can oblige WiFi operators to implement reasonable security measures, including password protection, to prevent the operator's network from becoming a haven for third-party infringement. This reinforces the principle that proportionate preventive measures short of complete blocking are an acceptable middle ground.

Synthesising these precedents, the CJEU framework requires the following: (i) the blocking order must target specific infringing content or platforms, not general monitoring; (ii) it must afford the ISP discretion in choosing technical means; (iii) it must strike a fair balance between the rights of the rightsholder, the freedom of information of users, and the legitimate interests of the service provider; and (iv) it remains the responsibility of national courts to assess proportionality and effectiveness in light of the concrete facts. Critically, the CJEU has never specified which blocking method is proportionate and which is not. That ambiguity is the root of the legal fragmentation discussed in the subsequent subsections.

### *2.3.3 The Open Internet Regulation: a second layer of constraint*

Website blocking orders operate in a second regulatory space defined by the Open Internet Regulation. Article 3(1) of the Regulation enshrines the right of end-users to access content of their choice. Article 3(3) prohibits ISPs from blocking, slowing, altering, restricting, degrading or otherwise discriminating against content, applications, services or network resources, except under three narrow exceptions. These exceptions are compliance with legal orders, network integrity and security, and network congestion management.

Website blocking orders, being backed by court judgments, fall under the legal order exception. Still, this does not exempt them from the proportionality requirement embedded in the same article. The BEREC Guidelines on implementation of the Open Internet Regulation, updated in 2022, provide detailed guidance to national regulators on how to assess whether a blocking order complies with Article 3(3). The Guidelines note that blocking orders issued in response to copyright infringement are generally consistent with the Open Internet Regulation, but they do not resolve a critical tension: a blocking order that is legally valid under copyright law as interpreted by the CJEU might still breach Article 3(3) if the blocking method employed is unnecessarily overinclusive.

A study by Ververis et al. (2024) examined website blocking orders through the lens of the Open Internet Regulation and found that several national implementations risk violating Article 3(3) through systematic overblocking. The authors argue that the definition of proportionality under copyright law and under net neutrality law should be harmonised.

Matthias Leistner's (2025) analysis, prepared in the context of an Austrian referral to the CJEU, argues forcefully that IP-based blocking is categorically disproportionate under Article 3(3) because it inevitably affects legitimate content. The Austrian regulatory authority, the TKK, found that IP blocking of this kind is inherently disproportionate, but Satel Film appealed. The Austrian *Bundesverwaltungsgericht* (the Austrian federal administrative court) then referred a number of questions to the CJEU under cases C-832/24, C-833/24, and C-834/24 late in 2024. Many had hoped that these cases would shed light on the CJEU's thinking, and might thus reshape national blocking regimes across the EU (see Section 2.4.3); however, Satel Film withdrew its case at the national level in March 2025. As a result, the TKK's decisions finding IP blocking to be disproportionate have become legally binding in Austria, yet no CJEU precedent has been established at EU level.

### *2.3.4 The Digital Services Act and the fragmentation problem*

The DSA, adopted in 2022 and now being implemented, was in part a legislative response to the fragmentation problem highlighted by earlier regulatory analyses. Recital 2 of the DSA explicitly recognises that divergent national laws governing online services create barriers to the single market. Article 9 of the DSA sets out a procedure and requirements for orders to act against illegal content, including provisions for cross-border coordination and due process.

All the same, the DSA does not harmonise copyright-specific blocking procedures. Instead, it establishes a procedural floor and a set of requirements for what must happen when an authority issues an order, while delegating substantive copyright questions to

the existing copyright framework (InfoSoc and Enforcement Directives, and national copyright law). This means that the 27 different national regimes established under copyright law remain in place, now topped with a DSA procedural layer. By late 2025, the European Commission had opened 14 investigations under the DSA, with the relationship between DSA compliance and national copyright blocking orders remaining an area of active regulatory development. Table 1 summarises key aspects of the current state of play.

Table 1. Key legal instruments at a glance

| Instrument | Year | Key provision |
|---|---|---|
| InfoSoc Directive (2001/29/EC) | 2001 | Art. 8(3): injunctions against intermediaries; conditions left to national law |
| Enforcement Directive (2004/48/EC) | 2004 | Art. 11: courts may order intermediaries to prevent/terminate IP infringement |
| Open Internet Regulation (2015/2120) | 2015 | Art. 3(3): blocking prohibited except under legal orders, with proportionality required |
| Digital Services Act (2022/2065) | 2022 | Art. 9: procedural requirements for content removal orders; does not harmonise copyright blocking |
| Satel Film (C-832–834/24) | Pending | A key test in Austria of the proportionality of IP-blocking under the Open Internet Regulation |

*Source*: Author's own elaboration.

## 2.4 COPYRIGHT: FRAGMENTED IMPLEMENTATION AT NATIONAL LEVEL

Legal fragmentation is visible in the six EU jurisdictions analysed below, plus the UK. Each has adopted a different approach to website blocking, reflecting different constitutional and procedural traditions, different copyright enforcement preferences, and different regulatory philosophies. For cross-border service providers, including VPN providers, CDN operators and DNS resolvers serving the entire EU-27, the result is a set of potentially incompatible compliance obligations.

### *2.4.1 Spain: private-entity delegation and fast-tracking*

In December 2024, a Barcelona commercial court granted LaLiga, the Spanish professional football league, the extraordinary power to specify IP addresses to be blocked by ISPs, with a list that LaLiga could update weekly without court approval. From February 2025 onwards, during match broadcasts, LaLiga targeted Cloudflare IP addresses known to host pirated streams. Because Cloudflare's IP addresses serve millions of legitimate domains through shared infrastructure, this resulted in the blocking of approximately 3 300 lawful services, including widely used platforms. The collateral damage was significant for ordinary users, businesses, and services that had no connection whatsoever to piracy.

The court dismissed a proportionality challenge in March 2025, and Cloudflare escalated the matter to Spain's Constitutional Court, arguing that the delegation of blocking authority to a private entity without ongoing judicial supervision violates the rule of law.

Spain also operates a parallel administrative enforcement track under Article 195 of the Copyright Act, under which the Copyright Commission within the Ministry of Culture can order site blocking for up to one year without prior judicial authorisation, based solely on a complaint from a rightsholder. This model is unusual in the EU. Most Member States require at least a judicial determination that infringement has occurred, even if the decision is made expeditiously.

### *2.4.2 Italy: administrative speed and systemic collateral damage*

Italy's Piracy Shield (Scudo Pirateria), operated by AGCOM[1], represents the most aggressively automated approach in the EU. ISPs are mandated to block notified domains and IP addresses within 30 minutes of AGCOM's notice. No court order precedes the blocking; AGCOM acts on the request of a rightsholder and the blocking is effective immediately, with the possibility of challenge only after the fact. As of January 2026, Piracy Shield had blocked approximately 65 000 domains and 14 000 IP addresses.

The collateral damage has been extensive and well documented. In February 2024, a single Cloudflare IP address serving millions of domains globally was inadvertently notified and blocked, effectively severing Italian users from a large swathe of the internet. In October 2024, a Google Drive domain was erroneously notified by a rightsholder, cutting off Italian users from their stored data for 12 hours until the mistake was corrected. These incidents have prompted the European Commission to intervene, citing concerns about DSA compliance, including the absence of prior judicial review, lack of transparency in the blocking list, and systemic overblocking. In January 2026, in an

[1] The technology was developed by Sp Tech, the technical arm of the Previti law firm, and donated to AGCOM by the Lega Serie A.

escalating dispute over Cloudflare's refusal to globally filter its 1.1.1.1 DNS resolver, AGCOM imposed a EUR 14.2 million fine on Cloudflare, prompting the company to threaten full withdrawal from the Italian market (Brodkin, 2026).

### *2.4.3 Austria: the proportionality frontier*

Austria potentially provided a test case for the proportionality debate in the EU that could have been important, but in the end, no EU-wide position emerged.

In 2022, Satel Film obtained a court order requiring Austrian ISPs to block domains and IP addresses associated with pirate streaming sites. The blocking was implemented through IP-level filters, meaning that any user attempting to connect to one of the blocked IP addresses would be redirected or refused. This approach is technically efficient and it catches any domain pointing to that IP, but it is inherently blunt (see Section 2.2.2). As a result, thousands of legitimate websites hosted on the same IP addresses as pirate sites became unavailable to Austrian users.

The Austrian TKK, the decision-making regulatory authority for electronic communications in Austria, ruled in August 2023 that IP-level blocking violates Article 3(3) of the Open Internet Regulation because overblocking is an unavoidable consequence, not a mere incidental effect. The TKK distinguished this from DNS-level blocking, which allows for more granular control at the domain level, and permitted DNS blocking to continue.

Satel Film appealed the TKK's decision, and the Austrian Federal Administrative Court referred the matter to the CJEU under cases C-832/24, C-833/24, and C-834/24. The case had been expected to provide CJEU guidance on whether the TKK's proportionality-based distinction between IP and DNS blocking should become an EU-wide standard, or national courts retain broader discretion; however, Satel Film chose to withdraw the case before the CJEU could rule.

### *2.4.4 Belgium: market exit as collateral damage*

In March 2025, DAZN obtained a Belgian court order requiring Google, Cloudflare, and OpenDNS to block nearly 100 pirate sports streaming domains. Critically, the order granted DAZN the freedom to unilaterally add new domains to the blocklist at will. Facing potential fines of EUR 100 000 per day for non-compliance, and unable to audit and verify the rapid domain additions requested by DAZN, OpenDNS withdrew entirely from Belgium in April 2025, leaving Belgian consumers without a key DNS security service.

The market exit was a disproportionate response to a disproportionate order. After negotiations with DAZN and Belgian authorities, OpenDNS returned in July 2025, but only after enforcement was suspended pending a more targeted review. The episode

illustrates how overreaching court orders can have unintended consequences for the broader digital ecosystem, and how disproportionate liability exposure can sometimes incentivise service provider withdrawal rather than compliance.

### *2.4.5 France: established judicial blocking*

France has one of the longest track records of website blocking in the EU, dating back to the Hadopi law of 2009 and refined through Article L.336-2 of the French Intellectual Property Code. The French approach is characterised by judicial oversight, specificity (targeting domain names rather than IP addresses when feasible), and a preference for DNS-level blocking over IP-level techniques. French courts have developed a body of relatively consistent case law on proportionality, and enforcement has been comparatively stable. The principal challenge for France going forward is scaling the model as piracy evolves and the volume of blocking orders increases, particularly for live sporting events.

However, the French landscape is evolving rapidly. Canal+ has pursued a systematic strategy of expanding blocking obligations to new categories of intermediaries: from traditional ISPs (2022) to alternative DNS providers such as Google, Cloudflare, and Cisco/OpenDNS (2024), to CDN and proxy services (2025), and most recently, to VPN providers. In May 2025, the Paris Judicial Court ordered five major VPN providers – NordVPN, Surfshark, CyberGhost, ExpressVPN, and Proton – to block 203 domains associated with unauthorised sports streaming, marking the first time VPN providers were recognised as 'technical intermediaries' under Article L.333-10 of the French Sports Code. Public DNS providers Cisco, Cloudflare, and Google were required to implement blocking measures on their DNS services; in consequence, Cisco withdrew its OpenDNS service from France entirely, reducing competition and consumer choice in the DNS market.

In February 2026, the Paris court issued three further judgments rejecting Cloudflare's defence that DNS, CDN, and proxy blocking would be technically impossible or disproportionate.

Several of these rulings are now subject to appeal before the Paris Court of Appeals specifically challenging the proportionality of the DNS and VPN blocking measures. The situation in France is therefore not settled but actively contested, and the outcomes of these appeals may significantly reshape the scope of permissible blocking in the EU.

Meanwhile, there is also a specific Sports Code in France directed at sports live events. Article L 333-10, I of the Sports Code provides that:

> Where serious and repeated infringements of the audiovisual exploitation rights provided for …, of the related rights of an audiovisual communication company …, where the program concerned consists of a sporting event or competition, or to a right acquired on an exclusive basis by contract or agreement for the audiovisual exploitation of a sporting competition or event, caused by the content of an online public communication service whose main purpose or one of whose main purposes is the unauthorized broadcasting of sporting competitions or events, and in order to prevent or remedy a further serious and irreparable infringement of those same rights, the holder of that right may apply to the president of the judicial court, ruling under the accelerated procedure on the merits or in summary proceedings, for the purpose of obtaining any proportionate measures to prevent or stop that infringement, against any person likely to contribute to remedying it.

### *2.4.6 Netherlands: proportionality review and judicial scrutiny*

The Netherlands experienced a landmark development in the *Stichting Brein* v *Ziggo* saga. The initial blocking order was granted by a Dutch court, but the Court of Appeals subsequently overturned it on proportionality grounds, finding that the scope of the blocking order exceeded what was necessary to protect copyright interests. The Dutch courts' willingness to revisit proportionality determinations is notable among EU jurisdictions. The case was then referred to the CJEU, which issued the C-610/15 judgment discussed above. The outcome in the Dutch courts was that blocking was reinstated, but with stricter parameters. The Netherlands thus represents a middle path: judicial blocking is permissible, but courts actively scrutinise scope and seek to avoid overreach.

### *2.4.7 United Kingdom: proportionality as a benchmark*

Although no longer part of the EU, the United Kingdom offers a valuable comparative benchmark. In *Sky* v *BT* and related cases, the English High Court has granted both static and dynamic blocking orders against ISPs, ordering them to block pirate streaming services. Critically, the High Court requires that the rightsholder bringing the action demonstrate with detailed technical evidence that the proposed blocking method will not block legitimate content more than strictly necessary. The court retains discretionary authority to reject the technical proposal, demand modifications, or impose conditions. Orders are explicitly time-limited, typically for two years, after which the court reassesses whether renewal is justified. Monitoring and reporting requirements seek to ensure that overblocking is detected and corrected.

The result is that the UK court-supervised reporting channel has recorded no noteworthy instances of significant overblocking. This might suggest that the collateral damage experienced in Spain, Italy, and Belgium is not an inevitable consequence of website

blocking, but rather a consequence of inadequate procedural safeguards. It should be noted, however, that overblocking can be difficult to detect. UK High Court orders include a clause permitting affected parties to apply to vary the order, but for smaller websites it may be practically impossible to determine that an access failure was caused by erroneous blocking, let alone to pursue a legal remedy. The absence of reported overblocking may therefore partly reflect detection and enforcement barriers rather than the complete absence of collateral effects.

As to the effectiveness in reducing piracy, the evidence is mixed. Danaher et al. (2020) analysed the UK blocking of Pirate Bay (2012) and subsequent waves of site blocking (19 sites in 2013, 53 in 2014), finding that blocking multiple piracy channels increased legal content consumption. A 2024 Digital Citizens Alliance study (Danaher, et al., 2024) found that traffic to blocked piracy sites in the UK had decreased by 89%. Yet, these measures capture traffic reductions to specifically blocked sites; whether overall piracy levels are declining is a separate and more complex question, as users may simply migrate to unblocked alternatives (see Section 3.2.4 on the evolution of piracy over time). Meanwhile, recent press coverage claims that the number of illegal streams of sports events in Britain has more than doubled in the past three years (Guardian, 2026).

## 2.5 CONSEQUENCES FOR CROSS-BORDER SERVICE PROVIDERS

The foregoing analysis exposes the acute problem faced by VPN providers, CDN operators, and DNS resolvers that serve not only the entire EU-27, but also a global user base. These global or pan-European services encounter not one blocking regime but 27, with conflicting procedural and substantive requirements. A single IP address block ordered by a Spanish court affects not just Spanish internet users but potentially disrupts service across Europe and globally. A domain blocklist maintained by an Italian regulator on a 30-minute timeline poses compliance risks to providers that cannot manually verify each addition in real time. A Belgian court order with unilateral domain-addition rights can trigger service provider exit. An Austrian determination that a particular blocking method violates net neutrality creates liability in that Member State yet not in others. An English court order imposes detailed monitoring and reporting obligations.

For these cross-border providers, the fragmentation creates an impossible choice. They must either accept blocking obligations that vary by Member State (creating operational complexity, legal risk, and the possibility of inadvertent non-compliance) or withdraw from certain markets, as OpenDNS did from both Belgium and France. The current incentive structure further exacerbates the misalignment: rightsholders bear none of the implementation costs and face no direct consequences for collateral damage caused by their blocking requests, with the burden falling entirely on service providers. This inverted cost allocation explains why overblocking is so pervasive, rightsholders have no incentive

to be conservative in their requests, and service providers have no effective tool to challenge the scope of a demand except by threatening withdrawal. The result is a race to the bottom in which the technical means of blocking become increasingly blunt and collateral damage escalates.

# 3. BENEFITS OF WEBSITE BLOCKING

### Key findings

- For illegal content or hybrid warfare content, the benefits of blocking seem clear. Copyright enforcement, however, raises different questions.
- Many experts would argue that overall copyright policy has totally run off the rails. Copyright was initially envisaged as a limited-time arrangement, with costs that need to be balanced against its negative impact on many forms of innovation.
- The European public acknowledges the overall value of the copyright regime at a philosophical level, if not at a practical or personal level. In a survey of more than 25 000 EU individuals conducted by the EUIPO in 2023, 93% see value in copyright protection; yet, 44% overall feel that strict protection of intellectual property constrains innovation, including 57% in the 15–24 age group.
- While 24% think that intellectual property enforcement benefits large companies, only 7% believe that it benefits SMEs. Only 8% see consumers like themselves as the main beneficiaries of intellectual property protection.
- In some (eastern) EU Member States, a majority feel that it is acceptable to obtain online content illegally when it is for personal use. Meanwhile, 48% of respondents aged 15–24 find it acceptable to access content illegally if it is only for personal use, compared with 27% of those aged 55–64 or 28% of those aged 65 and over.
- Some 14% of Europeans overall admit to having intentionally used illegal sources to access content online, while 33% of Europeans in the 15–24 age group admit to having done so. But this may be under-reported – some respondents may have been reluctant to 'out' themselves.
- Price and availability appear to play a huge role in the willingness to access content illegally. Among those who use online content from illegal sources, 43% report that lower prices might lead them to stop doing so; conversely, 44% report that the main reason they do not access content illegally is because the content they want is available via legal sources.
- The academic literature likewise strongly indicates a link between the level of piracy and the price, availability, and convenience of access to legal content.
- For illegal, on-demand, non-IPTV consumption of films, average consumption appears to have declined from 2.6 visits per internet user per month in January

2017 to 0.9 visits per month at the end of 2023, the latest available date for the data.

- For films and music, there is a wealth of solid, peer-reviewed research that supports the claim that the decline in illegal consumption can be attributed to increasing availability and decreasing prices over time. When content is available legally, on a timely basis and at a reasonable price, piracy drops. By contrast, lack of availability, delays (e.g. due to release windows), fragmentation among different content platforms, over-pricing, or inconvenience tend to drive an increase in piracy.
- Website blocking to prevent copyright infringement of audiovisual sports content simultaneously implies some of the greatest economic rewards and greatest risks of website overblocking.

In this chapter, we discuss the benefits of blocking illegal content, or hybrid warfare propaganda (Section 3.1), and material that allegedly infringes copyright (Section 3.2), which is our prime interest in this study.

## 3.1 ILLEGAL CONTENT AND HYBRID WARFARE PROPAGANDA

If one were to assume *arguendo* that website blocking is effective, then it would be hard to argue with the benefits of blocking of illegal content or hybrid warfare propaganda, or for that matter for the protection of minors. For harmful but legal content, however, the question is fraught.

Recital 12 of the DSA (Regulation (EU) 2022/2065) provides a lengthy catalogue of illegal content, while still leaving considerable scope for each Member State to expand on the definition of what constitutes illegal content.

> In order to achieve the objective of ensuring a safe, predictable and trustworthy online environment, for the purpose of this Regulation the concept of 'illegal content' should broadly reflect the existing rules in the offline environment. In particular, the concept of 'illegal content' should be defined broadly to cover information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities. Illustrative examples include the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer protection law, the nonauthorised use of copyright protected

> material, the illegal offer of accommodation services or the illegal sale of live animals. In contrast, an eyewitness video of a potential crime should not be considered to constitute illegal content, merely because it depicts an illegal act, where recording or disseminating such a video to the public is not illegal under national or Union law. In this regard, it is immaterial whether the illegality of the information or activity results from Union law or from national law that is in compliance with Union law and what the precise nature or subject matter is of the law in question.

The blocking of genuinely illegal content is relatively uncontroversial from a policy perspective, provided one assumes the blocking is effective and proportionate. Three important caveats nevertheless deserve emphasis in the context of this report.

First, the definition of what constitutes illegal content varies significantly by Member State. Material that is criminal in one jurisdiction may be merely distasteful in another. For example, sale of Nazi paraphernalia is a criminal offence in Germany but is protected speech in several other Member States. The DSA's broad catalogue of illegal content categories (Recital 12) deliberately leaves the determination of legality to each Member State. This divergence creates further fragmentation for cross-border service providers, which must navigate a patchwork of national definitions.

Second, for content that is harmful but legal, blocking engages Article 10 of the European Convention on Human Rights and Articles 11 and 52 of the EU Charter of Fundamental Rights. The proportionality threshold for restricting access to such content is high, and any blocking measure must be demonstrably necessary and proportionate to a legitimate aim.

Third, when it comes to blocking content, Article 3(3) of the Open Internet Regulation permits providers of electronic communications services to the public to block only subject to very limited circumstances (see Section 2.4.3). One of these is to abide by 'Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers'. A Council Recommendation is not, strictly speaking, an EU legislative act, and thus might not alone constitute sufficient grounds. Member State acts or court decisions to implement a Council Recommendation presumably qualify (Godlovitch, et al., 2023).

### *3.1.1 The EU's ban on Russian state media*

The most significant instance of content blocking for security purposes in recent EU history is the sanctions against Russian state media. On 2 March 2022, the Council adopted Regulation (EU) 2022/350, prohibiting the broadcast of RT and Sputnik through

all channels – television, radio, internet, and mobile applications – under Article 215 TFEU and Article 29 TEU. The CJEU upheld the sanctions, applying a four-part test: EU legal basis, respect for the essence of free expression, a general-interest objective, and proportionality. The sanctions have since been expanded to cover 32 outlets.

Enforcement, however, has been inconsistent. Reports indicate that RT and Sputnik websites remained accessible across much of the EU two years after the sanctions were imposed, because national audiovisual regulators responsible for implementation lack the technical capacity to monitor all online channels (PISM, 2024). The European Federation of Journalists opposed the measure on freedom-of-expression grounds, and Norway declined to implement it. These gaps illustrate a recurring lesson that is applicable far beyond the hybrid warfare context: a blocking order is only as effective as its enforcement mechanism.

The broader institutional context is also relevant. Under the DSA, the European Commission had opened 14 investigations by late 2025, and the European Democracy Shield package embeds content blocking within a wider framework including the AI Act, the European Media Freedom Act, and the Regulation on Transparency and Targeting of Political Advertising. Content blocking alone is insufficient to address hybrid warfare and foreign information manipulation; what matters is the institutional and procedural framework surrounding it. The legal basis for blocking hybrid warfare content under the Common Foreign and Security Policy should remain distinct from copyright blocking to prevent conflation of fundamentally different policy objectives.

## 3.2 PROTECTING RIGHTSHOLDERS AGAINST COPYRIGHT INFRINGEMENT/PIRACY

There is no question that intellectual property protection in general, and copyright protection in particular, are important pillars of innovation in the EU and worldwide. There is also no question that copyright protection is the law of the land, and must be enforced.

With that said, it is nonetheless important to reflect on the economic benefits and costs of copyright enforcement since they play a direct role in any assessment of the proportionality of website blocking to enforce copyright. Under multiple CJEU rulings, the question of proportionality is fundamental in assessing the permissibility of Member State website blocking rules.

It is useful here to distinguish between overall economic benefits of copyright protection of audiovisual content, versus benefits specific to the protection of sports content (which constitutes a special case).

### *3.2.1 Mixed economic benefits and costs of copyright law overall*

Many experts would argue that overall copyright policy has totally run off the rails. Copyright was initially envisaged as a limited-time arrangement. The Statute of Anne (1710) in the UK provided protection for just 14 years, with a possible 14-year renewal. After that, the work entered the public domain. Similarly, the US Constitution empowers Congress to 'promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries'. It followed the model of the Statute of Anne, allowing just 14 years of protection with the possibility of only a single renewal. That copyright today remains in effect for 70 years after the death of the last creator of the work has little to do with promoting creation, but rather with the enrichment of Hollywood studios. It is a political economy manifestation of the willingness of the studios to invest huge sums in lobbying to keep expanding their rights.

Beyond this well-known 'Mickey Mouse' phenomenon (the tongue-in-cheek claim that copyright will continue to be lengthened as long as needed to ensure that Mickey Mouse never becomes public domain), copyright is in obvious tension with EU competition law, as recent EU case law makes clear (Procee, et al., 2020). Geographical segmentation that would constitute a competition law violation in most contexts (especially in the case of passive sales) is permitted as an exception under copyright law (Procee, et al., 2020).

### *3.2.2 Attitudes in the EU to online copyright enforcement*

The limitations of copyright noted in Section 3.2.1 notwithstanding, the European public appears to acknowledge the overall value of the copyright regime at a philosophical, if not at a practical or personal level. In a survey of more than 25 000 EU individuals conducted by the EUIPO in 2023, 93% totally agree or tend to agree that 'it is important that inventors, publishers, creators and performing artists can protect their rights and be paid for their work' (EUIPO, 2023). On the other hand, 44% overall agree or tend to agree that strict protection of intellectual property hinders innovation, including 57% in the 15–24 age group. And while 24% think that intellectual property enforcement benefits large companies, only 7% believe that it benefits SMEs. Only 8% see consumers like themselves as the main beneficiaries of intellectual property protection (EUIPO, 2023).

This nuanced view of the value of intellectual property enforcement translates into a similarly nuanced view of whether individuals should respect intellectual property rights, and a view that varies considerably across EU Member States (see Figure 1) and by age group. In some (eastern) EU Member States, for instance, a majority feel that it is acceptable to obtain online content illegally when it is for personal use. Meanwhile, 48% of respondents aged 15–24 find it acceptable to access content illegally if it is only for

personal use, compared with 27% of those aged 55–64 or 28% of those aged 65 and over (EUIPO, 2023, p. 46).

Figure 1. To what extent do you agree that it is 'acceptable to obtain online content illegally when it is for your personal use'?


*Source*: EUIPO (2023, p. 46); n=25 824.

These differences in attitude translate directly into differences in conduct. Some 14% of Europeans overall admit to having intentionally used illegal sources to access content online, while 33% of Europeans in the 15–24 age group admit to having done so (EUIPO, 2023, p. 44). We caution, however, that this may be under-reported – some respondents may have been reluctant to 'out' themselves.

Price and availability appear to play a huge role in the willingness to access content illegally. Among Europeans who admitted to accessing content illegally, 61% also used paid legal sources. More specifically, 43% of those who use online content from illegal sources report that lower prices might lead them to stop doing so; conversely, 44% report that the main reason they do not access content illegally is because the content they want is available via legal sources (EUIPO, 2023, p. 44).

### *3.2.3 Benefits of enforcing copyright law for audiovisual sports content*

Sports should be understood to constitute something of a special case. Reasons include (i) the very high value that broadcast transmission media ascribe to audiovisual sports content; (ii) the high value that consumers place on such content, coupled with a desire to save money where possible; and (iii) the very rapid decline in the value of this content once the event has ended (Procee, et al., 2020).

Sports events as such are not protected by copyright or related rights in EU law, but the audiovisual recording of a sporting event can be protected by copyright. In the EU, rights are typically licensed based on exclusivity in a given time frame or a given geography. Meanwhile, the Audiovisual Media Services Directive empowers Member States to mandate the accessibility of certain designated events on free-to-air broadcasters, including a number of sports events. Sports events have been gradually shifting over many years from the major, general-interest television channels to premium sports channels and streaming equivalents, including SVoD and TVoD. This is a large and increasingly globalised business (Procee, et al., 2020).

The combination of factors specific to sports poses particular policy challenges. Sports are probably the area where website blocking offers greatest economic benefit, but only where the blocking is implemented very quickly. At the same time, the need for very rapid initiation of website blocking for audiovisual sports content implies a lack of sufficient time for due process controls to mitigate the risk of overblocking. In other words, website blocking to prevent copyright infringement of audiovisual sports content simultaneously implies both some of the greatest economic rewards and also some of the greatest risks of website blocking.

Sports have been a topic of intense interest at EU and Member State level, with specific legal measures in France (see Section 2.4.5) and a Commission Recommendation especially dealing with sports and events (European Commission, 2023).

### *3.2.4 Evolution of piracy over time*

The concern of rightsholders over piracy is understandable. A study by the EUIPO (Bornas Cayuela, Djail, & Wajsman, 2024) found substantial infringement of audiovisual content, and also of software, publications, and music.

The study is well done overall, but some unavoidable limitations must be taken into account. First, the EUIPO reports accesses per internet user per month, but this is really a multi-modal distribution, comprising some users who frequently view pirated content, and others who view pirated content rarely if at all. We noted in Section 3.2.2 that 14% (about a seventh) of Europeans admit to having used content illegally. If we take this

figure as given, it would suggest that the level of illegal consumption online of all types of content, reported by Bornas Cayuela, Djail, & Wajsman (2024) to be 10.2 accesses per internet user per month, is really composed of 70 accesses per month on average by those who consume illegal content, and none by those who do not.

The second limitation is that there is a huge gap in our knowledge of pirating of IPTV content, which should be understood to be a large component of online TV content overall. Data by a firm called Muso, which provides the basis of the analysis in Bornas Cayuela, Djail, & Wajsman (2024), can be assumed to do a good job of capturing visits to pirate websites; however, IPTV pirating functions differently – there may be a website visit when the user first subscribes, but not necessarily when content is viewed. 'IPTV piracy involves illegal streaming of TV, films, and live sports over Internet Protocol networks, sometimes mimicking legitimate IPTV services but bypassing official subscription channels. These pirated services often require specific hardware (boxes) or software (dedicated apps). They operate through subscription fees, advertising, or as a business-to-business model for resellers' (Bornas Cayuela, Djail, & Wajsman, 2024, p. 10).

The Muso data thus reflect visits to subscription sites for illegal IPTV content, but do not reflect actual use. Relatedly, not every visit to a subscription website results in an actual subscription. These limitations are honestly, fairly, and accurately acknowledged in Bornas Cayuela, Djail, & Wajsman (2024), but they must nonetheless be understood to be serious. They likely result in significant under-counting of online piracy, especially of sports, and also make it impractical to estimate trends over time.

In the past, online traffic data by Sandvine (e.g. of BitTorrent traffic) provided a useful cross-check on the Muso data. But Sandvine completely stopped reporting pirate traffic after 2020, largely because (i) it was increasingly common for the traffic to be encrypted (HTTPS or QUIC), and (ii) more generally, IPTV pirate traffic used various means (apps, boxes, and private channels) with no website visit after initial setup, and consequently could not readily be identified.

There is thus no reliable source of data on piracy of online audiovisual content today, since even the best sources are subject to a huge gap.

As regards piracy of music and on-demand films, the data in Bornas Cayuela, Djail, & Wajsman (2024) are presumably reliable, and a substantial decline is visible over time. For illegal on-demand consumption of films, average consumption appears to have declined from 2.6 visits per internet user per month in January 2017 to 0.9 visits per month at the end of 2023, the latest available date for the data (Bornas Cayuela, Djail, & Wajsman, 2024, p. 41).

For music, illegal on-demand average consumption appears to have declined from 2.6 visits per internet user per month in January 2017 to 0.6 visits per month at the end of 2023, the latest available date for the data (Bornas Cayuela, Djail, & Wajsman, 2024, p. 43). Once again, a substantial decline is visible over time. Differences among the Member States are conspicuous (see Figure 2).

For both films and music, there is a wealth of solid, peer-reviewed research that supports the claim that the decline in illegal consumption in recent years can be attributed to increasing availability and decreasing prices over time. When content is available legally, on a timely basis and at a reasonable price, piracy drops; conversely, lack of availability, delays (e.g. due to release windows), fragmentation among different content platforms, over-pricing, or inconvenience tend to drive an increase in piracy. We provide a few examples from a much larger stream of academic literature.

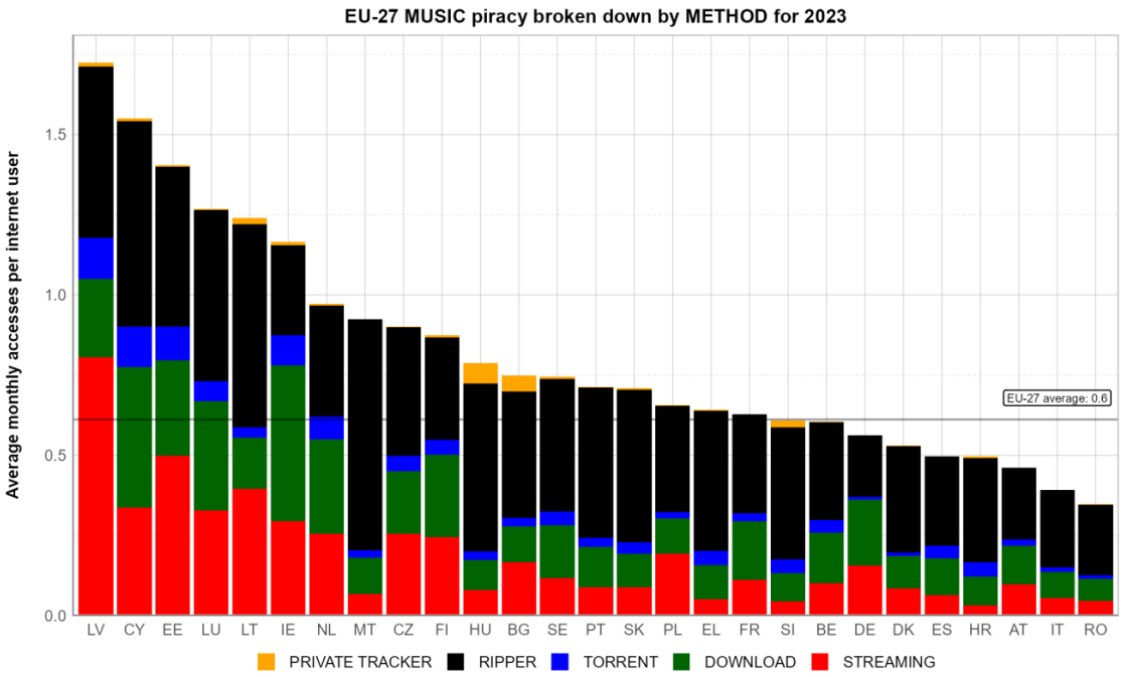
A well-respected meta-study of the literature (Danaher, Smith, & Telang, 2020) for the US Patent and Trademark Office found that

> firms can reduce piracy by making legal content more available and more appealing. Strategies such as making legal content available on convenient digital channels or reducing the release windows between different releases of the same product are both effective at changing consumption of pirated content. However, none of these strategies have been shown to reduce piracy by more than 25 percent. … [T]he most natural conclusion one can draw from the peer-reviewed literature is that the combination of firm strategies to make high quality legal content readily available and easy to use, and government and private actions to reduce the appeal of pirated content, is the most effective way to reduce piracy's impact on legal markets.

Another key study (Poort & Quintais, 2019) finds a 'strong link between piracy and the availability and affordability of content … [At] a country level, online piracy correlates remarkably strongly with a lack of purchasing power. Higher per capita income coincides with a lower number of pirates per legal [user].' It goes on to conclude that a clearly visible decline in piracy

> is linked primarily to increasing availability of affordable legal content rather than enforcement measures. Where content is available at affordable prices, in a convenient manner, and in sufficient diversity to address demand, consumers are willing to pay for it. This has significant policy implications, since it suggests that ongoing efforts to tackle illegal content online through repressive measures are misguided. Instead, it would make sense to direct resources towards enabling better lawful access to affordable content.

Figure 2. Illegal consumption of music online by Member State and method, 2023




*Source*: Bornas Cayuela, Djail, & Wajsman (2024, p. 43).

# 4. COSTS OF WEBSITE BLOCKING

## Key findings

- The practical effects of website blocking appear to be limited and may be short-lived because users are good at bypassing blockages, and pirate websites are good at migrating to unblocked venues.
- The burden of website blocking typically falls on parties other than those responsible for the infringement – notably on network operators, on providers of independent DNS resolution services, on providers of CDNs, or on providers of VPNs. The rightsholder does not bear the cost of the blockage.
- Website blocking regimes across the EU to date have consistently proven to be flawed and overly broad, owing to a combination of institutional shortcomings, technical limitations inherent to the blocking methods employed, and misaligned incentive structures.
- Near-real-time blockage precludes proper procedural safeguards to ensure that blockage is not overinclusive, and does not inappropriately impact freedom of expression.
- Measurement studies consistently show that illicit IPTV and live-streaming ecosystems are designed for rapid substitution through mirrors, alternative domains, and app-based delivery. Mirror sites can be located in countries that are uncooperative as regards copyright enforcement.
- As a result, academic literature tends to suggest that website blocking generates only limited and time-bounded positive effects, and that blocking is effective only when imposed on many websites at once, and in conjunction with expanding the availability and lowering the cost of legal alternatives.
- Danaher et al. (2023) found no consistent evidence of displacement of users from blocked illegal websites to unblocked illegal websites. But they found a fairly small yet statistically significant overall increase in consumption of legal content of 8.1%, 3.1%, and 5.2% in two blocking waves in India and one in Brazil, respectively.
- There are no current, reliable estimates of the longevity of the effects of website blocking.
- The measures in question here are being implemented at Member State level, but no two are alike. This could damage the EU single market. The risk that this fragmentation might pose undue burdens on cross-border operations has perhaps

been underestimated by Member State authorities, who do not themselves bear the costs, and also by EU policymakers, for whom the issue is not yet very visible.

- Blocking, if it is to be done at all, has to align with rules in the country of use rather than the country of origin.
- The Digital Services Act requires that the geographical scope must be as limited as possible (i.e. proportionate).

In this chapter, we consider the costs, limitations, and disadvantages associated with Member State website blocking measures, including the limited and time-bounded nature of their effects (Section 4.1), the burden on service providers (Section 4.2), the risks of collateral damage due to overblocking (Section 4.3), the risk to privacy and to freedom of expression (Section 4.4), and the negative impact on the EU single market (Section 4.5).

## 4.1 UNCERTAIN OR LIMITED EFFECTIVENESS OF MEASURES EMPLOYED

For the reasons identified in Section 2.2, one might expect the practical effects of website blocking to be short-lived and perhaps limited. Users are good at bypassing blockages, and pirate websites are good at migrating to unblocked venues.

In this section, we summarise the main results in the literature, distinguishing between earlier work (largely inspired by the blocking of Pirate Bay) and more recent results. Readers who want a more comprehensive and up-to-date review would do well to consult the literature review section in Danaher, et al. (2023).

Measurement studies consistently show that illicit IPTV and live-streaming ecosystems are designed for rapid substitution through mirrors, alternative domains, and app-based delivery. Mirror sites can be located in countries that are uncooperative on copyright enforcement. As a result, the technical impact of blocking is often short-lived unless blocking orders are continuously updated.

However, the behavioural duration of deterrence – how long users remain displaced or switch to legal services – has not been causally identified in recent literature. The absence of dynamic treatment-effect estimates means that policymakers should avoid assuming a specific 'half-life' of blocking effects for IPTV or live streaming.

Scholarly literature in the previous decade tended to suggest that website blocking generates only limited positive effects, and that blocking is effective only when imposed

on many websites at once, and in conjunction with expanding the availability and lowering the cost of legal alternatives.

This scepticism about the effectiveness of blocking is well expressed in Poort, van der Ham, & Dumitru (2014):

> The intervention can only affect consumers who download or intend to download from illegal sources, 27–28% over the past year. For this segment of the population, it is found that a large majority (70–72%) is non-responsive to blocking access to [Pirate Bay]. … For the small changes observed, it is not fully possible to disentangle the different and opposing effects of the blocking itself, awareness of the intervention, conversion to legal alternatives induced by the blocking, and a relapse as a result of circumvention or the launch of new file sharing platforms. … any behavioural change in response to blocking access to [Pirate Bay] has had no lasting net impact on the overall number of downloaders from illegal sources, as new consumers have started downloading from illegal sources and people learn to circumvent the blocking while new illegal sources may be launched, causing file sharing to increase again *(relapse effect).*

As regards the longevity of these effects, the authors go on to explain that there is

> a tendency found in the literature that any effects of legal action against file sharing often fade out after a period of typically six months, as the initial awareness effect wears off and illegal supply and demand find other places to meet. Probably, the required ICT knowledge to circumvent the blocking is no more advanced than the knowledge required to download from illegal sources. Hence, targeting individual file sharers and blocking access to file sharing platforms seem relatively ineffective to reduce unauthorised file sharing, while such measures bear a risk of alienating customers from the content industries and giving them incentives to adopt covert technologies such as dark nets, IP-spoofing and VPN.

These results are in line with Danaher, et al. (2020), who found that blocking only Pirate Bay in 2012 'caused no increase in usage of legal sites but instead caused users to increase visits to other unblocked piracy sites and VPN sites'. At the same time, they found 'that blocking 53 sites in 2014 caused treated users to decrease piracy and to increase their usage of legal subscription sites between 7% and 12%. It also caused an increase in new paid subscriptions.'

We note once again that these results should be interpreted with caution. Recent research confirms that blocking can sharply reduce access to targeted IPTV and streaming piracy services, but no study in the past five years provides a rigorous estimate of how long these effects persist. The alternatives available to consumers today are far different from those available when Pirate Bay was blocked back in 2012.

A comprehensive econometric analysis of the effects of website blocking in two waves in India and one in Brazil in 2019 through 2021 (Danaher, et al., 2023) found no consistent evidence of displacement of users from blocked illegal websites to unblocked illegal websites. They found a fairly small but statistically significant overall increase in consumption of legal content of 8.1%, 3.1%, and 5.2% in the two blocking waves in India and one in Brazil, respectively. Yet, when one considers only the change in behaviour for those who had been using the illegal websites before the blockage, the effect is much greater, constituting an increase of 48.3%, 53.6%, and 9.1%, respectively[2].

## 4.2 BURDEN ON SERVICE PROVIDERS

The burden on the entire ecosystem of internet intermediaries needs to be considered. At a time when the Draghi report (Draghi, 2024) cries out for reducing regulatory burden in order to bolster EU competitiveness, this cannot be ignored.

The costs borne by intermediary service providers can be substantial. At the operational level, compliance requires dedicated resources to receive, curate, and process blocking lists (often delivered outside business hours or at weekends under tight statutory deadlines such as the 30-minute implementation window under Italy's Piracy Shield). Each addition to a blocklist requires updating routing logic, verifying implementation, and monitoring for service impact. Where blocking regimes vary across jurisdictions in their technical requirements, providers may face the additional operational complexity, and also capital cost, of modifying or augmenting equipment to support jurisdiction-specific configurations that serve no purpose in their ordinary operations. Where a blocking measure causes collateral damage by rendering inaccessible a legitimate service, the provider faces user complaints, potential claims from affected third parties, and litigation exposure, despite having played no part in the underlying infringement. All of these costs are borne exclusively by the intermediary.

The burden of website blocking typically falls on parties other than those responsible for the infringement – notably on network operators, on providers of independent DNS resolution services, on providers of CDNs, or on providers of VPNs.

Those who impose these costs do not experience them directly. Proportionality is a key issue at EU level, and it is surely relevant here. To the extent that burdens are either out of proportion to the corresponding benefits, or that they fall on firms that should not have to bear them, this is a real concern. The burden of blocking in the country of use

[2] As the authors explain, the reason why the percentage impact in India is far greater than in Brazil can be explained by the fact 'that a much lower percent of Indian users were treated by the blocks (observed using the blocked piracy sites), while a large percent of Brazilian users were treated by the 2021 blocks'.

might fall to an ISP, a DNS provider, or a CDN or a VPN provider. The rightsholder does not bear the cost of the blockage.

## 4.3 FLAWED, OVERLY BROAD IMPLEMENTATION

Website blocking regimes across the EU to date have consistently proven to be flawed and overinclusive (see Section 2.4), owing to a combination of institutional shortcomings, technical limitations inherent to the blocking methods employed, and misaligned incentive structures.

There is reason to believe that at least some authorities are aware of the collateral damage their blocking measures cause. A key case arises from Italy's communications agency AGCOM. After numerous reports documented substantial overblocking by AGCOM's Piracy Shield system in 2024, AGCOM Commissioner Elisa Giomi issued two public statements criticising the system for 'unintentionally limiting freedom of expression' through overblocking. That blocking efforts continued despite such internal dissent suggests that awareness of the consequences does not necessarily translate into corrective action.

The technical means through which website blocking is implemented compound these institutional failures. IP blocking is the bluntest instrument, because tens or even hundreds of thousands of websites can share a single IP address, and blocking one address can render all of them inaccessible. Shared infrastructure can compound the risk – a blocked CDN resource could impact a great many otherwise unrelated sites simultaneously (see Section 2.2.2). The inverse problem is equally real – where anycast routing is used, as is common in CDNs, a single domain is served from multiple IP addresses across distributed nodes. Which address a user receives depends on which node is closest to them, meaning the IP address identified as serving infringing content may not be the address through which other users reach the same domain – leaving the targeted content fully accessible to them.

DNS blocking operates with greater precision, at the domain or subdomain level, but still risks collateral damage, particularly at the domain level. Additionally, DNS-level blocking can easily be defeated where users rely on encrypted DNS services. DPI is more targeted, but because it requires inspection of the content of data packets rather than just their metadata, it raises serious privacy concerns and may conflict with the General Data Protection Regulation and EU net neutrality rules. None of these methods can reliably restrict access to infringing content alone without affecting legitimate websites or user rights.

These problems are exacerbated by the fact that rightsholders bear none of the costs of website blocking and are thus incentivised to pursue stringent blocking orders without

concern for the collateral damage they cause – there is no back-pressure. The consequences of this dynamic are visible in the United States, where the low cost of filing takedown requests under the Digital Millennium Copyright Act has led rightsholders to submit requests to remove over 14.5 billion URLs from Google Search alone as of September 2025, many generated by automated systems with minimal human review that routinely catch legitimate content in the crossfire.

While this is specific to the US context, the underlying incentive problem is the same in the EU: when rightsholders do not bear the costs of enforcement, they have no reason to exercise restraint. Barring the UK's cost-indemnity approach, ISPs across Europe have generally been expected by courts to pay for the implementation of website blocking measures rather than rightsholders. Furthermore, rightsholders do not bear any cost that these measures might impose on freedom of expression (see Section 4.4).

Implementation at Member State level tends therefore to be flawed and overly broad because of a convergence of these factors: authorities that fail to act on known risks, technical methods that cannot achieve narrow targeting, and an incentive structure that insulates rightsholders from the consequences of excessive blocking.

## 4.4 RISKS TO FREEDOM OF EXPRESSION

Freedom of expression is becoming even more relevant today than in the past due to the increasingly tense geopolitical situation, and the breakdown in the transatlantic relationship. The EU has consistently sought to protect true freedom of expression.

The clear intent of the network neutrality provisions of the Open Internet Regulation is that users should have unrestricted access to all content, with only very limited exceptions. These Member State copyright infringement provisions potentially run counter to the spirit of that EU law.

Even where a single domain or a single IP address is blocked, and even where this targets only the intended entity, it is not necessarily the case that all content for that domain or address is illegal or infringing.

More generally, rightsholders are motivated to block as much as possible in order to enhance their profitability. It is up to policymakers to strike the right balance, ensuring that freedom of expression is guarded at the same time.

The duration of the block can also be an issue. Different Member States block IP addresses or domains for different periods – some only during a sports game, others for a whole season, which can be a year or more. That domain or IP address might continue to be blocked long after the grounds for the block have been addressed.

This implies an inherent tension. Near-real-time blockage might be optimal for enforcement, but it precludes proper procedural safeguards to ensure that blockage is not overly broad, and does not inappropriately impact freedom of expression.

## 4.5 EXTRATERRITORIAL OVERREACH

Infringing content will often be hosted in a different country from that in which a blocking order is sought. Moreover, a pirate site might well have mirror sites in multiple countries.

There have been calls to block illegal content at the source. A fundamental challenge, however, is that what is illegal in one jurisdiction is not necessarily illegal in the country where a website is based. Adult content that is legal in most or all EU Member States might be illegal in some Arab countries. Copyright is likewise subject to some national variability – the US recognises fair use, but not the EU; the EU has a text and data mining provision in the Copyright Directive from 2019, with no exact US counterpart.

This seems to suggest that blocking, if it is to be done at all, has to align with rules in the country of use rather than the country of origin. But many of the technologies currently involved in website blocking (including VPNs) are ill-suited to providing blocks with sufficient granularity.

Unlike ISPs, which are licensed national or regional operators with dedicated local networks and infrastructure within a defined (usually national) territory, global providers such as VPN providers operate distributed infrastructure spanning dozens of countries, where the same physical infrastructure simultaneously serves users across multiple jurisdictions. This means that global providers have no native mechanism for applying a measure solely to users in one country, while leaving service to users in all other countries unaffected.

At the same time, Article 9(b) of the DSA is explicit in calling for a clearly defined geographical scope, as limited as possible, for any blocking orders:

> Member States shall ensure that when an order … is transmitted to the provider… [the] order contains the following elements: … the territorial scope of that order, on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, is limited to what is strictly necessary to achieve its objective.

The principle of proportionality that is so visible in CJEU decisions is thus explicitly codified in the DSA in terms of geographical scope.

## 4.6 EFFECTS OF FRAGMENTATION ON THE EU SINGLE MARKET

The laws in question here are being implemented at Member State level, but no two are alike. The risk that this fragmentation might pose undue burdens on cross-border operations has perhaps been underestimated by Member State authorities, who do not themselves bear the costs, and also by EU policymakers, for whom the issue is not yet very visible.

Recital 2 of the DSA makes clear that divergent laws on illegal content or disinformation are detrimental to the single market, and very much the same concerns can be viewed as being relevant to website blocking of copyrighted material as well.

> Member States are increasingly introducing, or are considering introducing, national laws on the matters covered by this Regulation, imposing, in particular, diligence requirements for providers of intermediary services as regards the way they should tackle illegal content, online disinformation or other societal risks. Those diverging national laws negatively affect the internal market, which, pursuant to Article 26 of the Treaty on the Functioning of the European Union (TFEU), comprises an area without internal frontiers in which the free movement of goods and services and freedom of establishment are ensured, taking into account the inherently cross-border nature of the internet, which is generally used to provide those services.

This burden manifests most notably on cross-border service providers and cross-border merchants (see Section 2.5).

# 5. IMPLICATIONS OF THE FINDINGS: RECOMMENDATIONS

First and most importantly, we would argue that the excessive focus on blocking ignores other measures that could be undertaken, including by the rightsholders themselves. The approach taken so far by the EU, Member States, and the rightsholders has concentrated on one set of enforcement tools, without paying sufficient attention to other approaches that are probably more effective in the longer term, and with fewer negative side effects. Policy to date has centred on limiting the *supply* of infringing content, without giving due consideration to the *demand* for infringing content, mainly because the current approach is painless for the rightsholders.

A study by the EUIPO has stated this clearly. 'Enforcement is challenging due to technological sophistication, jurisdictional issues and consumer demand for cheap content. … [*A*] *multifaceted approach involving technology, legal efforts, and education is essential to combat this issue effectively*' (emphasis added) (Bornas Cayuela, Djail, & Wajsman, 2024, p. 10).

## 5.1 PRICE REDUCTIONS AND INCREASED AVAILABILITY

An important tool is in the hands of the rightsholders themselves. As noted in Section 3.2.2, EUIPO survey data indicate that 43% of Europeans who use online content from illegal sources report that lower prices might lead them to stop doing so, while 44% report that the main reason they do not access content illegally is because the content they want is available via legal sources.

The literature strongly suggests that website blocking can be effective only as part of a comprehensive programme, and only in conjunction with lowering prices and expanding availability (see Section 4.1).

The European Commission has argued along the same lines. Paragraph 33 of its Recommendation on combating online piracy of sports and other live events states: 'Holders of rights in live transmissions of sports and other events should be encouraged to increase the availability, affordability, and attractiveness of their commercial offers to end users across the Union' (European Commission, 2023).

In principle, the rightsholders should be in the best position to judge how to price their offerings. With that said, there are reasons to suspect that current pricing levels are not optimal even for the rightsholders. Consumer price elasticity of demand[3] for streamed content is surprisingly high – lower prices should be associated with an increase in demand that is more than sufficient to make up the difference (White, 2025). But any

[3] This is the way in which consumers buy more, or less, of a good or service in response to a change in its price.

shift in this direction would need to be carefully planned, since the price elasticity appears to be asymmetric – consumer willingness to subscribe in response to price reductions is less than consumer willingness to cancel a subscription, or to shift to alternatives (e.g. advertising-based) in response to price increases.

Relatedly, the industry practice of geo-blocking (limiting availability of online copyrighted content to a single country or a single group of countries based on language) means that high-value content is not legally available to some consumers who want it, and who are willing to go to great lengths to obtain it. The EU has enacted a law to prevent certain forms of geo-blocking, but audiovisual content has been completely excluded, largely in response to concerns on the part of rightsholders that doing so would reduce their margins and thus lead to less new content being produced. More recent work, including our own and that by Procee, et al. (2020), suggests that these concerns were substantially overstated.

Furthermore, the fragmentation of rights across multiple platforms, especially for sports, results in inconvenience for consumers and massive de facto over-pricing. The owner of a Spanish LaLiga 2 team recently posted that he

> pays for four DAZN subscriptions, plus Movistar, Amazon Prime, and probably something else I'm forgetting, just so my family and I can watch our matches. Yet when I travel outside Spain or Europe, it's often impossible to watch our games. … Even in Spain, … [there] isn't currently a simple standalone option for fans who just want to follow their team or league. In today's economic climate, affordability and flexibility matter. If we want to continue growing and addressing piracy in a meaningful way, I would humbly suggest that exploring more accessible and convenient viewing options for supporters could be an important step forward. (Voulgaris, 2026)

When one considers the combined effects of increased consumption due to a price elasticity response, together with reduced piracy, we think that rightsholders would be well advised to reflect seriously on their current pricing structures. There is good reason to think that a reduction in over-pricing might be advantageous to many rightsholders.

- Recommendation 1. Rightsholders would be well advised to reflect on their pricing schemes and on any restrictions on availability and convenience (including fragmentation across multiple platforms, together with geo-blocking) that they impose. The most effective means of combating piracy would be to ensure widespread availability of affordable content. The gains in reduced piracy should be evaluated together with gains from an increase in consumption in light of the high elasticity of consumer demand for content.

## 5.2 USER EDUCATION

Raising user awareness should also play a role. EUIPO survey data suggest that some 90% of users are aware of legal offers, and that many users take pains to avoid using infringing content (Bornas Cayuela, Djail, & Wajsman, 2024). Still, a large fraction of users is sometimes uncertain as to whether the offer that they are accessing is in fact legal.

The European Commission's Recommendation on combating online piracy of sports and other live events states in paragraph 34:

> Member States are encouraged to raise users' awareness on legal offers of live sports and other events. Member States are also invited to inform users who try to access services offering unauthorised retransmission of live sports and other live events, which had been blocked pursuant to an injunction, about the reasons for the blocking and provide them with information about the legal offers available for watching such events. (European Commission, 2023)

- Recommendation 2. Measures to assist users in distinguishing legal from illegal content, including improved education, should be part of any comprehensive strategy to combat online piracy.

## 5.3 REMEDIATION AT THE MOST APPROPRIATE LEVEL

In terms of remedying the problems of illegal content, the philosophy of Recitals 27 through 29 of the Digital Services Act should play as large a role as possible. We think that they should be understood to be relevant to infringing content too.

Recital 27 specifically explains that responsibility for dealing with illegal content rests with the actor that is responsible for the harm while acknowledging that effective legal remedies will not always be available. Read in context, Recital 27 says that the party that posted the illegal content '… should be held liable, where the applicable rules of Union and national law determining such liability so provide, for the illegal content that they provide and may disseminate to the public through intermediary services.' In other words, the infringer – the party that reproduces and distributes protected content without the rightsholder's authorisation – is the first and most appropriate target of any remediation.

As noted elsewhere in this study, some content will be hosted in a different country from that where it is used. The content might be permissible in the country of origin, but illegal in the country of use. Providers of pirated content will naturally prefer to host such content in countries that are lax in enforcing intellectual property rights. It is the country of use that has unambiguous ability to enforce its rules, including rules regarding copyright.

If the content is hosted in a lax or uncooperative country outside the EU, there are likely to be legal and practical considerations that might either limit the ability to take action against the infringing party, or that potentially introduce delay.

This implies a particular challenge for providers of global services, inasmuch as they might be obliged to block content in one or more countries where it is prohibited, but to provide services for the same content in countries where it is permissible. For a provider of a global service, this might be quite a feat.

Aside from that, seeking to block infringement at the source will not necessarily prove to be a panacea. It is more likely to simply change the way in which infringers choose to operate. Furthermore, where legitimate providers are caught in enforcement battles that lead to overblocking and deterioration in service quality, users may switch to services in countries with lax enforcement, exposing themselves to additional risks, including weakened security protections.

Recital 27 goes on to say that 'other actors … should also help', presumably only when it is not possible to solve the problem through measures targeting the infringing party. We think that this should be understood to mean that measures against intermediaries should only be considered where action against the infringer has failed or is not feasible. Where action against the infringer is feasible, proceeding directly against intermediaries without first seeking relief against the infringer risks imposing a disproportionate burden on parties whose role in the infringement is, at most, indirect, and is inconsistent with the principle of proportionality.

- Recommendation 3. Whether content is illegal or infringing needs to be judged for the purpose of blocking under the laws of the country of use, not those of the country of origin.
- Recommendation 4. Whenever legally and practically feasible, rightsholders should first pursue infringers who reproduce their content without consent before addressing intermediaries.

### 5.4 HARMONISATION AND CONSISTENT SAFEGUARDS FOR BLOCKING PROCEDURES

The analysis in Section 2.4 demonstrates that the fragmentation of national blocking regimes constitutes a major structural problem. Cross-border service providers face 27 different sets of procedural and substantive requirements, creating legal uncertainty, operational complexity, and perverse incentives that drive overblocking.

Guidance at EU level to date has been limited, for instance, to a recommendation dealing with sports and events (European Commission, 2023). More detailed EU guidance is called for.

- Recommendation 5. Additional guidance at EU level on whether to block, and if so, then how, is called for, taking into account the principle of subsidiarity, the need to avoid fragmentation of the EU single market, and the growing need to avoid unnecessary burden on the sector (including on intermediaries that have little or nothing to do with any infringing content).

In terms of the process followed, any EU guidance should address four priorities.

First, blocking orders should be subject to prior or rapid judicial review. The Italian Piracy Shield model, under which blocking occurs within 30 minutes of an administrative notification without prior judicial assessment, has produced the most documented instances of overblocking and collateral damage in the EU. Administrative speed should not come at the expense of fundamental procedural safeguards.

- Recommendation 6. Blocking orders should be subject to prior or rapid judicial review.

Second, IP-based blocking should be avoided altogether due to its scant effectiveness, together with the high risk of collateral damage (blocking legitimate content together with infringing content). To the extent that blocking is used at all, better targeted mechanisms such as DNS-level or URL-level blocking should be used instead, consistent with the Austrian TKK's reasoning. IP-based blocking is inherently overinclusive because shared IP addresses serve thousands or millions of legitimate domains.

- Recommendation 7. IP-based blocking should be avoided altogether. To the extent that blocking is used at all, better targeted mechanisms such as DNS-level or URL-level blocking should be used instead.

Third, delegation of blocking authority to private entities, as practised in Spain and Belgium, should be accompanied by meaningful oversight and safeguards, including against the risk of harm to fundamental freedoms like the freedom of expression. The Spanish model, under which LaLiga unilaterally specifies IP addresses to be blocked without ongoing judicial supervision, and the Belgian model, under which DAZN could add domains to a blocklist at will, are incompatible with the rule of law and the proportionality principle as articulated by the CJEU.

- Recommendation 8. Any delegation of blocking authority to private entities must be accompanied by meaningful oversight and safeguards.

Fourth, blocking orders should be time-limited with periodic review, following the UK model. The English High Court's practice of issuing two-year orders subject to renewal review, with monitoring and reporting requirements, has produced a blocking regime that is both effective against piracy and compatible with proportionality. This approach should be adopted as a minimum standard across the EU-27.

In line with Article 9(b) of the DSA, the geographical scope of any order must be clearly identified.

- Recommendation 9. Blocking orders should be time-limited with periodic review, and the geographical scope should be clearly defined and limited as much as possible.

### 5.5 COST ALLOCATION AND LIABILITY FOR OVERBLOCKING

The current incentive structure, in which rightsholders bear none of the implementation costs and face no consequences for collateral damage caused by their blocking requests, is a structural driver of overblocking. Rightsholders have no economic incentive to be conservative in the scope of their requests, and service providers have no effective means of challenging the breadth of a demand except by threatening withdrawal from the market, as OpenDNS did from Belgium and France.

A number of reforms could be considered to better align incentives. For a start, rightsholders should be required to contribute to the costs of implementing blocking measures, proportionate to the scale and complexity of the blocking requested. Furthermore, rightsholders should bear liability for damages caused by overblocking, creating a financial incentive to target blocking requests narrowly. Finally, the EU should consider adopting a cost-indemnity model similar to the UK system, under which the rightsholder bringing the action bears the compliance costs imposed on the intermediary.

More generally, rightsholders could be doing more to protect their content, for instance by means of watermarking or Digital Rights Management protections.

- Recommendation 10. Reforms should be considered to better align incentives. Rightsholders should be required to contribute to the costs of implementing blocking measures, proportionate to the scale and complexity of the blocking requested, and they should bear liability for damages caused by overblocking implemented at their request.

## 5.6 NET NEUTRALITY COMPLIANCE

National regulators should be required to assess blocking orders for compliance with Article 3(3) of the Open Internet Regulation before implementation, not merely after the fact. The Austrian TKK's approach of distinguishing blocking methods by their overblocking risk represents current best practice, and this approach should be endorsed as a model for other national regulatory authorities.

- Recommendation 11. As part of their proportionality assessment, national regulators should assess blocking orders for compliance with Article 3(3) of the Open Internet Regulation before implementation, not merely after the fact.

## 5.7 THE BLOCKING OF HYBRID WARFARE CONTENT

The experience of the EU's ban on RT and Sputnik reveals the need for clearer Council guidance on what content to block and how, to prevent the enforcement confusion experienced by network operators after the 2022 sanctions. Two years after the sanctions were imposed, RT and Sputnik remained accessible across much of the EU, demonstrating that a blocking order without an adequate enforcement infrastructure is insufficient.

The legal basis for the blocking of hybrid warfare content under the Common Foreign and Security Policy should remain clearly distinct from copyright blocking to prevent conflation of fundamentally different policy objectives. Enforcement coordination should be strengthened, and national regulators should be provided with sufficient technical capacity and clear guidance to ensure consistent implementation across the EU-27.

- Recommendation 12. Enforcement and coordination of the blocking of hybrid warfare content should be strengthened, and national regulators should be provided with sufficient technical capacity and clear guidance to ensure consistent implementation across the EU-27.

## 5.8 SUMMARY OF THE RECOMMENDATIONS

A brief recap of our recommendations follows, together with the page number on which each recommendation appears along with substantiation for its need.

Recommendation 1. Rightsholders would be well advised to reflect on their pricing schemes and on any restrictions on availability and convenience (including fragmentation across multiple platforms, together with geo-blocking) that they impose. The most effective means of combating piracy would be to ensure widespread availability of affordable content. The gains in reduced piracy should be evaluated together with gains

# BIBLIOGRAPHY

Abecassis, D., Daly, A., & Glickman, D. (2025). *The economic cost of network blocking.* Analy<sys Mason.

Bornas Cayuela, D., Djail, A., & Wajsman, N. (2024). *Online Copyright Infringement in the European Union: Films, Music, Publications, Software and TV (2017-2023).* European Union Intellectual Property Office (EUIPO). doi:10.2814/3685063

Brodkin, J. (2026, March 18). *Cloudflare appeals Piracy Shield fine, hopes to kill Italy's site-blocking law*. Retrieved from Ars Technica: https://arstechnica.com/tech-policy/2026/03/cloudflare-appeals-piracy-shield-fine-hopes-to-kill-italys-site-blocking-law/

Danaher, B., Hersh, J., Smith, M. D., & Telang, R. (2020). THE EFFECT OF PIRACY WEBSITE BLOCKING ON CONSUMER BEHAVIOR. *MIS Quarterly*, 631-659.

Danaher, B., Hersh, J., Smith, M., & Teland, R. (2020). The Effect of Piracy Website Blocking on Consumer Behavior. *MIS Quarterly*.

Danaher, B., Sivan, L., Smith, M. D., & Telang, R. (2024). The Impact of Online Piracy Website Blocking on Legal Media Consumption.

Danaher, B., Sivan, L., Smith, M., & Teland, R. (2023). *The Impact of Piracy Website Blocking on Legal Media Consumption.*

Danaher, B., Smith, M., & Telang, R. (2020). *Piracy Landscape Study: Analysis of Existing and Emerging Research Relevant to Intellectual Property Rights (IPR) Enforcement of Commercial-Scale Piracy.* U.S. Patent and Trademark Office (USPTO).

Draghi, M. (2024). Retrieved from https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2024/04/16/20240416%20Speech%20Mario%20Draghi%20La%20Hulpe%2016%20April%202024.pdf

EUIPO. (2021). *Study on Dynamic Blocking Injunctions in the European Union.* EUIPO.

EUIPO. (2023). *European Citizens And Intellectual Property: Perception, Awareness, and Behaviour - 2023.* EUIPO. doi:10.2814/87818

European Commission. (2023). *Commission Recommendation of 4.5.2023 on combating online piracy of sports and other live events.*

Ferri, F. (2021). The dark side(s) of the EU Directive on copyright and related rights in the Digital Single Market. *China-EU Law Journal* , 21-38.

Godlovitch, I., Wiewiorra, L., Kroon, P., Eltges, F., Marcus, J., Hocepied, C., . . . Firth, B. (2023). *Study on the implementation of the open internet access provisions of Regulation 2015/2120", stud.*

Guardian. (2026). Sports piracy explodes in UK with 3.6bn illegal streams and rise of black-market bookmakers. Retrieved from https://www.theguardian.com/sport/2026/jan/15/sports-piracy-explodes-uk-illegal-streams-black-market-bookmakers?CMP=Share_iOSApp_Other

Hagg, e. a. (2021). Retrieved from https://eur04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fstockholmiplawreview.com%2Fwp-content%2Fuploads%2F2022%2F01%2FThe-effectiveness-of-blocking-injunctions-against-ISPs_IP_nr-2_2021_A4.pdf&data=05%7C02%7Cjulien.libert%40ceps.eu%7C8b0ef153e12

ICANN. (2025). *DNS Blocking Revisited.* ICANN. Retrieved from https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac127-dns-blocking-revisited-16-05-2025-en.pdf

Leistner, M. (2025). The First SEP/FRAND Decisions on the Merits of the UPC – An Overview in Context.

Letta, E. (2024). *Much More than a Market: Speed, Security, Solidarity.* European Commission. Retrieved from https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

Marcus, J. (2024). *How to achieve better EU laws.* CEPS.

Marcus, J., & Rossi, M. (2024). *Strengthening EU digital competitiveness Stoking the engine.* EUI Centre for a Digital Society. EUI/RSC Centre for a Digital Society. Retrieved from https://cadmus.eui.eu/handle/1814/76877

PISM. (2024). *PISM Bulletin No. 78 (2386)*. Retrieved from https://eur04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fpism.pl%2Fwebroot%2Fupload%2Ffiles%2FBiuletyn%2FPISM%2520Bulletin%2520no%252078%2520(2386)%252028%2520May%25202024.pdf&data=05%7C02%7Cjulien.libert%40ceps.eu%7C8b0ef153e12441a9514f08de95619

Poort, J. J., van der Ham, J., & Dumitru, C. (2014). Baywatch: Two approaches to measure the effects of blocking access to The Pirate Bay. *Telecommunications Policy 38*, 383–392.

Poort, J., & Quintais, J. (2019). The Decline of Online Piracy: How Markets – Not Enforcement – Drive Down Copyright Infringement. *American University International Law Review, 34*(4; Article 5). Retrieved from https://digitalcommons.wcl.american.edu/auilr/vol34/iss4/5

Procee, R., Arnold, R., Marcus, J., Fina, D., Lennartz, J., Kazakova, S., & Lykogianni, E. (2020). *Study on the impacts of the extension of the scope of the Geoblocking Regulation to audiovisual and non-audiovisual services giving access to copyright protected content.* European Commission.

Renda, A., Simonelli, F., Mazziotti, G., A., B., & Luchetta, R. (2015). *The Implementation, Application and Effects of the EU Directive on Copyright in the Information Society.* CEPS. Retrieved from https://cdn.ceps.eu/wp-content/uploads/2015/11/SR120_0.pdf

Ververis, V., Lasota, L., Ermakova, T., & Fabian, B. (2024). Website blocking in the European Union: Network interference from the perspective of Open Internet. *Policy & Internet*, 121-148.

Voulgaris, H. (2026). Retrieved from Reddit: https://www.reddit.com/r/soccer/comments/1rbo6qj/voulgaris_i_own_a_la_liga_2_club_and_pay_for_four/?share_id=uXkylPbQODed-RJBhwDZ6&utm_content=1&utm_medium=android_app&utm_name=androidcss&utm_source=share&utm_term=1

White, N. (2025, June 16). *Consumers slash TV streaming subscriptions as price sensitivity peaks*. Retrieved from https://www.askattest.com/blog/research/consumers-slash-tv-streaming-subscriptions-as-price-sensitivity-peaks

Zenner, K., Marcus, J., & Sekut, K. (2025). *Overview of EU legislation in the digital sector.* CEPS. Retrieved from https://www.ceps.eu/ceps-publications/a-dataset-of-international-legal-and-policy-instruments-for-the-digital-world/

Zornetta, A. (2024). Harmonization or Further Fragmentation? The EU's Approach to the Protection of Copyright Online.

CEPS
PLACE DU CONGRES 1
B-1000 BRUSSELS