Anti-Piracy strategies

CONCERNING CULTURAL AND SPORTS CONTENT IN FRANCE AND ABROAD

SUMMARY • 2019 - 2020 INTERNATIONAL SURVEY

Hadopi

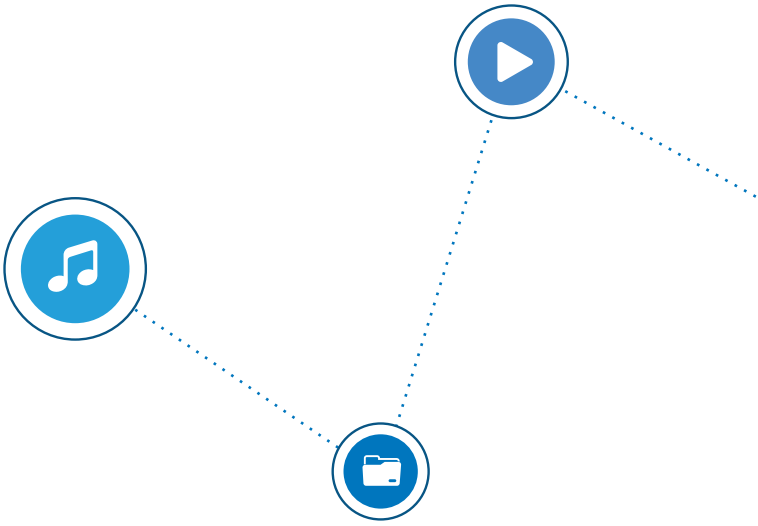
High Authority for the Dissemination of Works and the Protection of Rights on the Internet

METHODOLOGY

- Monitoring of anti-piracy actions internationally has been carried out continuously by Hadopi's Legal, European and International Affairs Department since 2011 and is published for the third time. This new edition includes new developments that Hadopi became aware of during the period from January 2019 to January 2021.

- The international survey includes a summary of the highlights and current issues in the fight against piracy, referencing the most emblematic national systems, as well as appendices containing detailed fact sheets for each of the 32 countries studied. For the first time, in order to meet the expectations of Hadopi's international readership, a fact sheet is devoted to France.

- This work was carried out thanks to the international network of contacts established by Hadopi over the years. Hadopi would like to thank all its contacts, in particular the International Federation of the Phonographic Industry (IFPI) and the Motion Picture Association (MPA).



ENHANCED INTERNATIONAL COOPERATION CALLING FOR GENUINE INTERNATIONAL COMPETENCE OF PUBLIC AUTHORITIES

The transnational nature of the piracy phenomenon and illegal actors, as well as the similarity of the challenges to be overcome by each of the countries affected, calls for a strengthening of international alliances.

The monitoring work carried out by Hadopi has enabled it to acquire recognised expertise in France and internationally in the fight against piracy, under which it regularly exchanges with both private players involved in the fight against piracy worldwide and with the local public authorities or international bodies concerned.

In 2019 and 2020, Hadopi continued its relations with the European authorities and, in particular, with the European Observatory on Infringements of Intellectual Property Rights managed by the European Union Intellectual Property Office (EUIPO)[1]. The work of the Observatory is based in particular on a network of specialised contacts from the public sector, private groups or civil society within the various Member States of the European Union, which meet in four thematic working groups. Since 2018, Hadopi has officially represented France in the "Intellectual property in the digital world" working group.

[1] The EUIPO is a decentralised agency of the European Union, created to protect the intellectual property rights of companies and creators. Since 2012, the EUIPO has hosted the European Observatory on Infringements of Intellectual Property Rights, whose mission is to provide data and tools to support the fight against infringements of intellectual property rights.

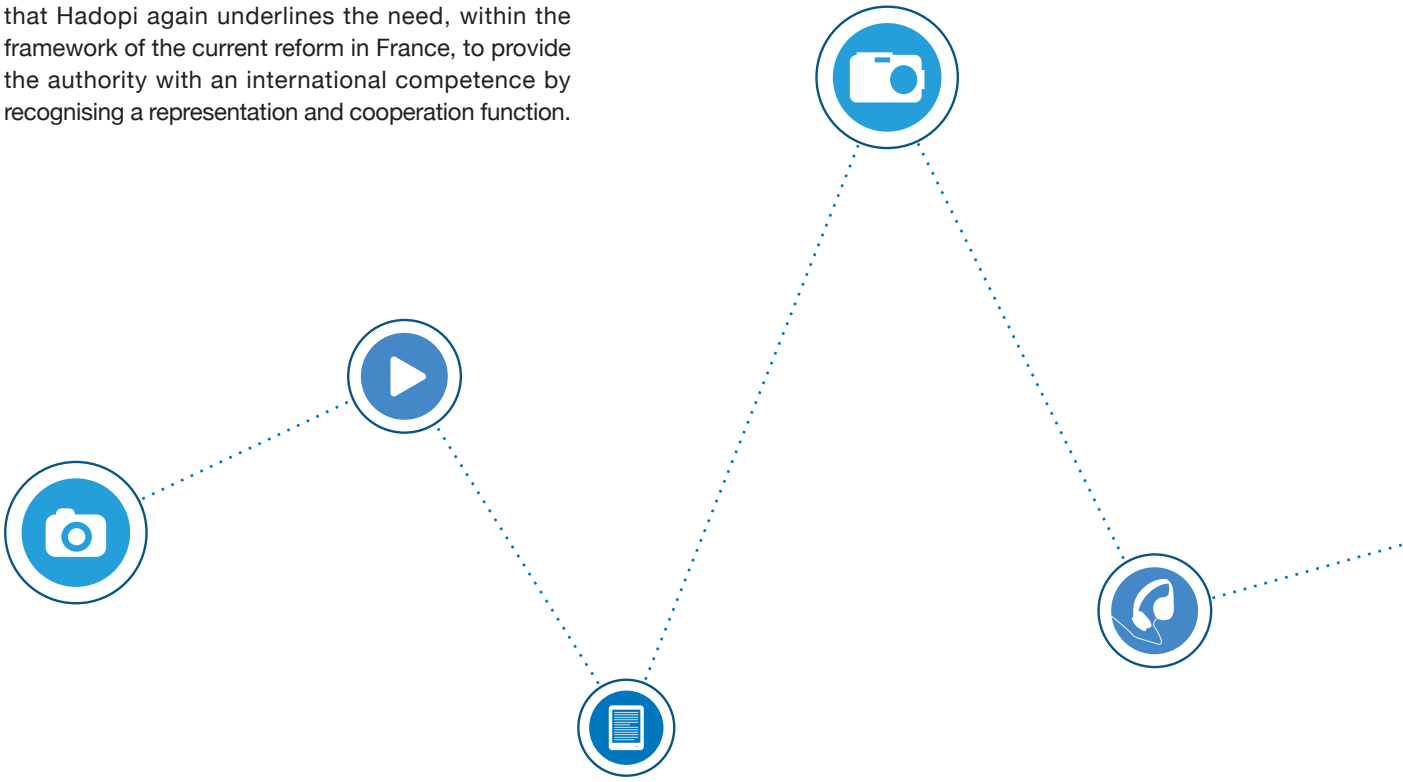
In addition, Hadopi is a stakeholder in the network developed by the EUIPO, entitled “Intellectual property in education”, consisting of representatives from ministries of education, national offices and other public sector players, as well as representatives from teachers and European schools. The network supports the education community, bringing intellectual property closer to the classroom through practical and interactive initiatives to raise awareness of the value of intellectual property for both students and teachers. Lastly, Hadopi agents are also members of the “Cooperation with intermediaries” and “Impact of technologies” expert groups set up by the Observatory since January 2019. Complementary to working groups, these expert groups are intended to explore topics addressed in working groups or to report topics identified as of particular interest.

Since 2017, Hadopi has also been in discussions with the World Intellectual Property Organization (WIPO), a specialized agency of the United Nations, regarding the “WIPO ALERT” system. As part of this new tool aimed at cutting off the financial resources of infringing websites resulting from advertising, WIPO is proposing to the authorised bodies of the Member States, first and foremost the public authorities, to contribute to a centralised database listing infringing websites worldwide. This database is then made available to online advertising players.

It is in light of these collaborations and exchanges that Hadopi again underlines the need, within the framework of the current reform in France, to provide the authority with an international competence by recognising a representation and cooperation function.

Cooperation between national regulatory authorities at the European level, as already exists with regard to the regulation of audiovisual media, electronic communications or the protection of personal data, is currently a strong link in the implementation and application of regulations at the European level.

The proposed Digital Services Act (DSA) regulation published in December 2020, which aims to update the legal framework currently in force for digital services, and in particular certain provisions of the so-called “e-commerce” Directive, provides for the strengthening of the role of national authorities in the regulation of digital services in collaboration with European institutions, with in particular the creation of a local Digital Services Coordinator who will be specifically responsible for the application of the regulation. Thus, this regulator will be responsible in particular for issuing a “trusted flagger” status label, which could potentially include right holders in the cultural and sports sector. This status requires that platforms first process their notifications.



USING PUBLIC AUTHORITIES TO OVERCOME DIFFICULTIES IN CHARACTERISING MULTIFACETED AND EVOLVING ILLEGAL OFFER

An analysis of the services targeted by the actions of audiovisual and music right holders reveals that these have evolved significantly in recent times, in line with changing uses.

Initially, right holders mainly targeted sites providing links to content available for download or streaming.

Today, we can see that services of a varied nature are appearing (applications, devices dedicated to piracy, etc.) and are gaining in popularity, thus requiring actions against them:

- audiovisual right holders are currently particularly affected by services illegally streaming television channels (so-called illegal IPTV services). They are also acting against the various actors in the ecosystem of illicit streaming devices enabling users to pirate audiovisual content;

- with regard to actions undertaken by the music industry, stream ripping services that make illegal content available to their users are now the main target of international right holders, measures targeting these services having recently been implemented for the first time in many countries.

Recently, several successful actions have also been brought against cyberlockers both by the music industry and by audiovisual players (particularly in France, Italy and Russia), even though these services are not editorialized and it is therefore often considered difficult to take action against them, in particular due to the limited liability regime of hosting providers.

In some countries, the criteria for qualifying sites as illegal are predefined by law, case law or the administration (particularly in Canada, Lithuania, Portugal and Singapore). In most cases, a body of evidence is created that can include in particular a system of thresholds (the number of works or links in question) or the percentage of illegal content identified.

To ensure that proposed measures against illegal websites do not become obsolescent, ineffective (or even inapplicable), the assumptions and criteria used to qualify a site or service as illegal should be quite flexible.

It is therefore now a matter of facilitating and accelerating the designation of the various players in the fight against piracy as illegal, in order to make the task of right holders and the courts easier.

This area of improvement is first and foremost crucial at the national level to facilitate and streamline the use of blocking measures and measures taking the so-called “Follow the money” approach, and also at the international level. Actually, since the blocking of a site is ordered by the competent local authority for the national territory alone, if the right holders wish to obtain blocking measures against the same site in another country, they will need to gather the evidence required in this other country to have its blocking ordered.

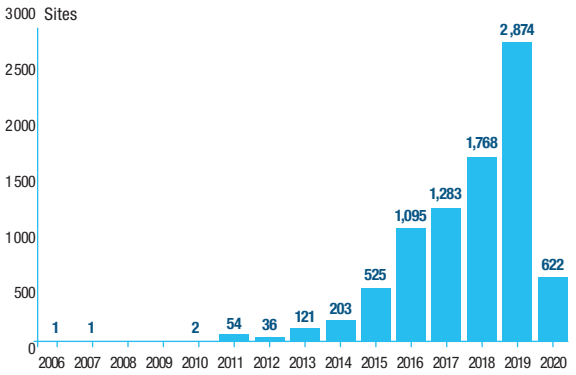
Therefore, the question arises, in particular at the European level, of the consideration by the judicial or public authority of a given country of previous judicial or administrative decisions handed down in a third country concerning the same site. The implementation of “Follow the money” measures at the European and especially the global level through the system created by WIPO also calls for increased intervention by public authorities regarding the classification of illegal sites.

THE NEED FOR A FLEXIBLE AND AGILE SYSTEM TO COMBAT STRATEGIES TO CIRCUMVENT BLOCKING MEASURES IMPLEMENTED BY OPERATORS OF ILLEGAL SERVICES

Throughout the world, the very generic expression of “mirror site” has emerged, which encompasses in a very heterogeneous manner the phenomena of reappearance and replication of blocked sites as well as the creation of misappropriated access to these sites. These practices of circumventing measures implemented against them by the administrators of illegal sites highlight the extent of piracy and the need to find an agile solution to allow blocking measures to retain their effects over time.

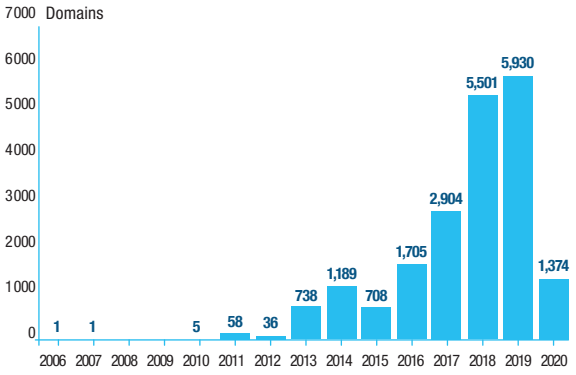
The figures below illustrate the fact that today, on average, for each illegal service blocked, at least two domain names relating to this service must be blocked.

FIGURE 1 : TOTAL NUMBER OF SITES BLOCKED EACH YEAR



Source : *Motion Picture Association - June 2020*

FIGURE 2 : TOTAL NUMBER OF DOMAIN NAMES BLOCKED EACH YEAR



Source : *Motion Picture Association - June 2020*

Both public authorities and case law - particularly at European Union level[2] - agree that blocking measures, although circumventable, have a considerable impact on the ecosystem. In addition, several studies have concluded that blocking measures are effective as they generally lead to an approximately 75% drop in visits to blocked sites.[3].

In countries that implement administrative or judicial blocking measures on a large scale, it seems that in most cases blocking results directly in the digital death of the target site. According to some, 30 % to 40% of blocked sites reappear.

However, the collateral effects of the blocking measures identified in France are on the one hand the fragmentation of the illegal offer through a myriad of small sites with smaller capacity and audiences, the audience of illegal sites no longer concentrated on a few large sites with a very high reputation, and on the other hand, the very strong dynamic of illegal sites that seek to circumvent the blocking measures through the proliferation of avatars.

It appears that while updating of the blocking measures taken by public authorities is generally quite simple (in Greece, Italy, Lithuania Russia and Spain), with regard to judicial blocking orders, their updating increasingly involves so-called dynamic injunctions which themselves provide for the procedures for their updating and are often accompanied by voluntary agreements between right holders and Internet service providers (in particular in Australia, Canada and Denmark, India, Ireland, in the United Kingdom, Singapore and Sweden). In France, a hybrid solution is under study and could involve an optional use of the intervention of the public authority to secure and define the framework within which the updating of blocking measures ordered by the courts takes place.

[2] CJEU, 27 March 2014, C-314-12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH.
[3] In particular: www.incoproip.com/report/site-blocking-efficacy-report-australia www.incoproip.com/news/portugals-pirate-site-blocking-system-works-great-study-shows www.incoproip.com/report/site-blocking-efficacy-study-united-kingdom papers.ssrn.com/sol3/papers.cfm?abstract_id=2612063

THE INVOLVEMENT OF SO-CALLED ALTERNATIVE DNS TO COMBAT THE CIRCUMVENTION OF BLOCKING MEASURES BY WEB USERS

The Domain Name System, or DNS, is a key web system that provides the correspondence between the domain name of a site and the address of the server where this site is hosted. Subscribers of an Internet service provider use by default the DNS service that it makes available to them. When this Internet service provider implements a domain name blocking measure (known as DNS blocking), it generally configures its DNS service so as to provide users with an invalid hosting address for the site to be blocked or so as to redirect connections to a substitute server (which for example displays an alert or information message).

Discussions are currently underway (particularly in Italy and Lithuania) to further involve DNS services that are used by internet users to circumvent DNS site blocking by choosing a so-called “alternative” DNS service to that of their internet service provider, for example that offered by Google or Cloudflare.

These considerations are all the more important as the effectiveness of blocking measures is likely to be reduced by the recent development of DNS over HTTPS (DoH) – a technical development of the DNS system which aims to improve the security and level of protection of users’ privacy, by encrypting exchanges between Internet users’ applications or equipment and DNS servers. Indeed, the use of DoH most often actually involves the use of an alternative DNS service. However, its use could quickly become widespread because it can be proposed by default, or through simple configuration by browsers, operating systems or an internet box.

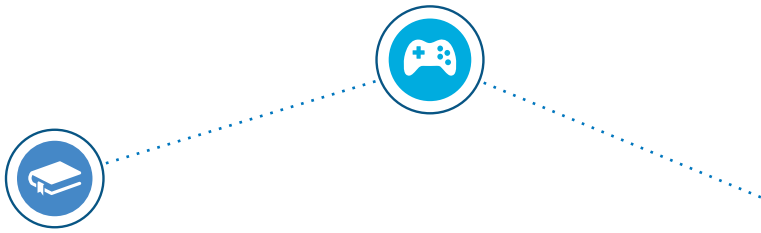
Among the avenues envisaged to avoid the circumvention of DNS blocking measures, subject to the proportionality of these measures with regard to the level of use of these services, is the possibility of requiring the DNS blocking of illegal sites not only to internet access providers but also to operators offering alternative DNS services, with all the procedural difficulties involved in bringing an action against a player who is often based abroad. In Italy, the local public authority entered into a voluntary agreement concerning CISCO DNS service in 2019. Under its terms, CISCO has undertaken to block, for Internet users using its service from Italy, the sites covered by a blocking order issued by the local public authority, AGCOM, intended solely for local Internet service providers.

Recital 27 of the aforementioned DSA proposal lists Internet intermediaries that currently exist but were not expressly covered by the text of the so-called “e-commerce” Directive, including domain name systems. It is stated that these players may benefit from the liability regime for technical intermediaries if it is possible to link them to one of the categories provided for by the Directive and supported by the proposed regulation, namely services offering infrastructure network, cache services and hosting providers. Therefore, although the DSA confirms the possibility of obtaining cessation measures within the European Union against domain name system services, it would be very useful, however, for it to expressly specify the status of alternative DNS.

THE NEED TO CREATE A SPECIFIC MECHANISM TO FIGHT AGAINST PIRACY OF SPORTS MATCHES

The specific characteristic of sports piracy is that, unlike audiovisual works such as cinema or TV series, the economic value of a sporting event expires once it ends.

This is why it is essential that anti-piracy measures be adapted for this type of dissemination, so that protective measures can be taken very quickly during sporting competitions. This practice is referred to as “live blocking”.



Worldwide

In its international survey published in 2019, Hadopi highlighted several administrative and judicial models of live blocking of services pirating sports content, in particular in the United Kingdom (judicial IP blocking) and in Portugal (administrative DNS blocking).

Since then, it has emerged that new countries have acted against the piracy of sports content:

- there has been case law involving issuance of DNS blocking measures for sports piracy in new countries (Denmark, Spain, India, Singapore);
- the English model of live temporary IP blocking has been used in Ireland and Portugal, where there is also an administrative system for live DNS blocking;
- administrative injunctions were issued in Peru and Vietnam.

In France

A study published by Hadopi in May 2019 indicates that 24% of web users watch live programmes illegally[4]. With regard more specifically to sports content, a study published by Hadopi and the French Audiovisual Council (CSA) in March 2020 estimates that 17% of web users watch illegal online sports programmes[5].

However, the organisers of sporting events do not, under current law in France, have any *ad hoc* legal proceedings to directly obtain blocking and delisting measures from Internet service providers or search engines in the event of piracy of their content.

Drawing on these lessons, the French anti-piracy reform project plans to create a system to combat the piracy of live sports matches to obtain blocking measures adapted to live streaming.

[4] https://www.hadopi.fr/ressources/etudes/etude-la-consommation-illicite-de-programmes-tv-en-direct
[5] https://www.hadopi.fr/ressources/etudes/la-diffusion-du-sport-sur-internet-un-marche-et-des-usages-en-developpement-etude

INVOLVEMENT OF THE VARIOUS INTERMEDIARIES IN THE FIGHT AGAINST PIRACY

The pervasive, multifaceted nature of piracy means that a wide variety of tools and strategies are needed to prevent it. It also calls for the involvement of all digital actors, which cannot go on avoiding - either through indifference or inertia - the challenges associated with the profusion of illegal online content. Some players, particularly in the advertising sector and to a certain extent search engines, have committed to an active approach to combating counterfeiting.

In order to combat piracy even more effectively and to ask each of the technical intermediaries in the Internet ecosystem to be equally involved in the fight against piracy, it is now necessary to consider extending this approach of involving intermediaries to other actors such as domain name registrars and hosting service providers, in order to ensure that they can suspend the domain names of massively infringing sites or cease hosting them.

Involving hosting service providers

The updating of the legislative framework in light of the current challenges seems to be gaining consensus in Europe, since Directive 2000/31/EC of 8 June 2000, known as the "e-commerce" Directive, has not achieved all its objectives and is insufficient to meet the new challenges related to digital transformation, and the European Commission has presented the aforementioned DSA proposal.

This proposal shows that the main principles of the so-called e-commerce Directive have not really been completely changed, merely developed and made more specific, in particular with regard to hosting providers.

Regarding the notice and take-down system, a standardised, accessible and user-friendly mechanism must be put in place by all hosting providers, without imposing a processing time frame on them.

However, the time frame for the removal of illegal content by hosting services is one of the key factors in the fight against the piracy of sports content.

Proposals in this regard are currently being discussed in the European Parliament, with a view to asking the Commission to submit a legislative proposal, at the heart of which could be the proposals made by the European Parliament consisting of introducing dynamic injunctions and take-down measures within a time frame appropriate to live streaming (in real time or 30 minutes).

Finally, as things stand, the DSA has not complied with the right holders' request known as "*Know your customer*", promoted in particular by the *Motion Picture Association*, consisting of requiring technical intermediaries, and in particular hosting service providers, to implement a proportionate and effective protocol to verify the identity of their customers on the basis of validated documents, data or information (such as registration of the company or any other sufficient proof of identity). An obligation to this effect appears in the DSA proposal but it only concerns marketplaces – and therefore above all trademark holders.

Involving search engines

While the involvement of search engines increasingly takes the form of agreements concluded as part of a voluntary approach, where applicable under the aegis of the public authority (in particular in Australia, France, Japan, the United Kingdom and Russia), the question may however arise, and in particular in the context of the Digital Services Act proposal, regarding the creation of a liability regime specific to search engines with enhanced obligations in terms of the delisting of illegal sites – and in particular in the context of the updating of blocking measures ordered by the court or the public authority – or even demotion of the illegal offer.

Traffic optimisation services or content delivery networks

Content delivery network (CDN) services provide their customers with network infrastructure capable of optimising the delivery of content to users, in particular when the service's customers are domiciled in different countries. These services are used by both legal and illegal players and in particular by players disseminating audiovisual content in quantity, a bandwidth-intensive operation that justifies the use of CDN services. One of the most important CDNs in this sector is the US-based technical operator Cloudflare, whose services are used by many infringing sites – but also by lawful services.

This operator, in addition to its CDN services, also offers several technical services including a so-called "reverse proxy" service (which centralises all incoming or outgoing connections from/to a site, which makes it possible to hide the IP address and the identity of the true host of a site). The anonymisation of illegal sites that may result from the use of Cloudflare considerably

hinders anti-piracy operations because it obfuscates the precise location of websites.

As such, Cloudflare was included on the first list of physical and digital markets reported to the European Commission as infringing or facilitating the infringement of intellectual property rights – the "*Counterfeit and Piracy markets watch list*" – published by the European Commission in December 2018. The second list, published in December 2020, no longer lists Cloudflare among the illegal actors and invites CDNs and right holders to cooperate more in order to help facilitate the enforcement of rights violated by CDN clients.

In the context of the *Digital Services Act*, in view of the role played by CDNs and the multiplicity of services they offer, the question arises of encouraging these players to combat the use of their services for illegal purposes through different means, such as for example the possibility of implementing geographical blocking measures for sites recognised as illegal; the communication of the IP address of sites to public authorities and recognised private sector organisations within time frames and under conditions that permit an effective fight against illegal sites. Recital 27 of the *Digital Services Act* only specifies that content delivery networks may benefit from the same liability regime as other technical intermediaries, provided that it is possible to link them to one of the categories provided for in this legislation, namely services offering network infrastructure, cache services and hosting providers. It can therefore be deduced that measures may be taken against them, but there are already calls to request that their status and obligations be expressly clarified, for all their activities and in particular those known as *reverse proxy*.

Involving online advertising players

While there is widespread consensus on the utility of measures to identify and cut off the funding sources of infringing sites (based on the "Follow the money" approach), questions are now being raised about their implementation, impact and effectiveness.

Consideration should be given not only to optimising and securing existing arrangements, but also to extending them to involve actors other than intermediaries, such as domain name registrars, hosting providers and search engines, thereby enabling them respectively to suspend the domain names of massively infringing sites, stop hosting them, or demote them.

Public intervention is provided for in an increasing number of countries to more effectively guarantee the reliability and control of sites subject to measures to cut off their income stream, and to better assess the impact and effectiveness of such measures (namely in Brazil, Denmark, India, Spain and the United Kingdom).

It is also important to note the initiatives aimed at extending the effects of this tool internationally such as the "Memorandum of Understanding on Online Advertising and IPR" (MoU) signed at the European level on 25 June 2018 by online advertising players under the aegis of the European Commission, which invited in particular to provide for restrictions and safeguards to prevent private players from being considered as arbiters of the infringing nature of the sites. It also emerges from the report published in August 2020 by the European Commission on the first year of implementation of this agreement, that the actions implemented under the agreement could in the future be carried out in cooperation with national or international authorities responsible for drawing up lists of illegal services. More recently, WIPO launched the "WIPO ALERT" system, which offers authorised bodies in Member States the opportunity to contribute to a centralised database listing the infringing websites identified worldwide, which will be made available to online advertising players.

Finally, while the actions undertaken under the "Follow the money" approach may be based on lists of illegal services, the establishment of such lists may also have a stigmatising function known as "Name and Shame". This approach, implemented by the United States and the European Union, consists of drawing up public lists of illegal services with

the aim of stigmatising bad actors or economic markets. Although one of the objectives of these lists is to conduct advocacy actions with regard to the countries in which listed services are domiciled, it also aims at involving all digital players (illegal services covered by the lists as well as their business partners) and raise awareness among end users regarding the risks inherent in using the services listed.

Involving online content-sharing platforms

Given their audience and the multiplicity of content they disseminate under a limited liability regime, platforms are a key element in a successful policy to combat piracy.

For several years, their development has raised questions with the public authorities about the regulatory framework to be applied to these new players in order to establish a healthy competitive playing field while respecting the specificities of the Internet.

In competition with services such as music or audiovisual streaming service publishers, these players question the very foundations of copyright and related rights, which are notably intended to allow their holders to authorise – by negotiating the terms – or on the contrary to prohibit the use of their works and protected subject matters.

Faced with this situation, the adoption of Article 17 of Directive 2019/790 of 17 April 2019 constitutes a major advance for the enforcement of copyright and the dissemination of works in the digital world by clarifying the liability regime for content sharing platforms. It is now provided that content sharing providers, by giving public access to a large number of protected works and subject matters, carry out an act of communication to the public or of making content available for which they must obtain authorisation from right holders or, in the absence of such authorisation, must make their "best effort" to prevent these protected works and subject matters being available on their service.

This new framework gives full place to content recognition technologies, which, provided that right holders have provided the fingerprints of their works, allow them to be detected automatically and then to manage, more or less automatically, how they should be handled under agreements entered into with right holders.

Member States have until 7 June 2021 to adopt the laws, regulations and administrative provisions necessary to comply with this Directive. At the same time, the European Commission is working, in cooperation with Member States, to examine best practices for cooperation between online content-sharing service providers and right holders.

Beyond the European initiative, there are initiatives or discussions in some countries to develop a provision with objectives similar to those of Article 17 (in particular in India, the United States, Russia and Vietnam).

All studies are on
www.hadopi.fr

Conatct us :
presse@hadopi.fr

Publishing Director:
Monique Zerbib-Chemla

Contributors to this issue:
Mathilde Persuy, Delphine Liotard and Carla Menaldi

Hadopi Publications:
Communication mission

Publication:
AGENCEZEERA.COM

May 2021

HIGH AUTHORITY FOR THE DISSEMINATION OF WORKS AND THE PROTECTION OF RIGHTS ON THE INTERNET

4 rue du Texel - 75014 Paris - France
www.hadopi.fr

Hadopi