Arcom

The Regulatory Authority for
Audiovisual and Digital Communication

REPORT

Assessment of technical measures for identifying protected works and objects implemented by online content sharing service providers

April 2023

Contents

Summary & Recommendations

Article 17 of Directive 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market introduced a specific authorisation and liability mechanism for copyright and related rights that applies to certain online content-sharing service providers. It is now recognised that online content-sharing services perform an act of communication to the public when they give the public access to copyright-protected works or other protected subject matter uploaded by their users.

The Directive's incorporation into French legislation by the Government order no. 2021-580 of 12 May 2021[1] settled in Article L. 137-2 of the French Intellectual Property Code (IPC) a liability exemption mechanism for service providers. Therefore, if no authorisation is granted by the rightholders, "*online content-sharing service provider shall be liable for unauthorised acts of exploitation (...), unless it demonstrates that it has fulfilled all the following conditions:*
(a) It made its best efforts to obtain an authorisation from the rightholders who wish to grant such authorisation;
(b) It made, in accordance with high industry standards of professional diligence, its best efforts to ensure the unavailability of specific works for which the rightholders have provided the service providers with the relevant and necessary information, whether directly or indirectly through a third party
(c) It has in any event acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from his service, the notified works, and made best efforts to prevent their future uploads in accordance with point b".

In addition, Article 17 of the Directive of 17 April 2019 includes measures for users, which have been incorporated into Article L. 137-4 of the French Intellectual Property Code. This article enunciates the new provisions "shall not prevent the free use of the work to the extent permitted by the rights provided for in this code, as well as those granted by the rightholders". Users may not be deprived of the "effective benefit" of the exceptions to copyright and related rights. Finally, the code specifies that online content-sharing service providers are required to implement a system allowing users to dispute a decision to remove or block content, and allow for a further appeal to be lodged with the Audiovisual and Digital Communications Regulator (Arcom).

Law no. 2021-1382 of 25 October 2021 on the regulation and protection of access to cultural works in the digital age supplemented these provisions by entrusting Arcom with a mission to **evaluate the level of effectiveness of the measures with regard to their ability to ensure the protection of works and protected objects** as described in Article L. 331-18 of the IPC. This article also empowers Arcom to **encourage cooperation between rightholders and online content-sharing service providers** with a view to **ensuring the availability of the content uploaded by users, which does not infringe copyright and related rights**.

---

[1] French Regulation no. 2021-580 of 12 May 2021 incorporating Article 2(6) and Articles 17 to 23 of Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

In this context, Arcom launched a consultation with the parties involved – content sharing service providers and rightsholders – by publishing two questionnaires[2] on its website from April 28 to July 13, 2022.

The questionnaires were designed to ask service providers and rightholders about the protection measures implemented and especially the application of legal provisions, agreements to authorise or block content between service providers and rightholders, and the various tools and measures proposed by service providers for reporting works and ensuring their unavailability. The aim was also to specifically gather feedback from rightholders about the solutions available.

This report provides a summary of the main responses to the questionnaires and presents the evaluation by rightsholders of the tools made available by content-sharing service providers.

It also relies on the transparency reports from these service providers and aims to understand the entire system, going beyond just the evaluation of the content recognition technologies.

By the end of the first year in which these provisions became effective, it appears that the content-sharing service providers who answered the questionnaire have generally complied with the provisions of Article L. 137-2 of the IPC.

After consulting the relevant stakeholders, Arcom notes that content-sharing service providers have taken measures to ensure that works are unavailable where no prior authorisation has been obtained from rightholders by using existing content recognition tools or developing new tools. These tools are mainly based on the fingerprinting technology and tend to be effective, although there is room for improvement. On this particular point, Arcom notes that service providers and rightholders need to regularly discuss the operation and use of these tools to ensure that they are understood and used more effectively.

As far as disabling access to notified works or removing notified works is concerned, Arcom draws attention to the effectiveness of the mechanisms that the service providers have implemented, including content recognition tools and takedown notice forms. However, the visibility of the takedown notice forms could be improved.

Regarding the agreements aimed at authorizing or controlling the use of works and determining access conditions to the tools, Arcom observes that the majority of these agreements are primarily established by the largest service providers (Meta, TikTok, YouTube) and rightsholders from the audiovisual and music sectors. It appears necessary for all service providers to commit to better cooperation with all rights holders by expanding the scope covered by these agreements to include all cultural sectors, especially photography and publishing.

Furthermore, Arcom encourages rightsholders and service providers to provide more information that would enable them to promote cooperation between rights holders and online content sharing service providers. The aim is to ensure the availability of user-uploaded content on the service that does not infringe on copyright and related rights.

---

[2] Available in the appendix.

Summary of Arcom's recommendations

Content-sharing service providers could:

With regard to rightholders:

(Recommendation 1) Improve information towards rightholders of any sectors regarding recognition tools at their disposal;

(Recommendation 2) Propose training courses or give access to tutorials to rightholders, even through collective management organisations, in order to help them to master recognition tools;

(Recommendation 3) Set up simplified tools for rightholders who do not have the technical and economic resources to use complex tools;

(Recommendation 4) Make content management systems (CMS) easier to use and supplement the management options offered.

With regard to users:

(Recommendation 5) Mention the applicable copyright rules and provide information on the situations in which exceptions to copyright can be made;

(Recommendation 6) ease access to reporting forms, in particular by ensuring better visibility and free access to them;

(Recommendation 7) inform French users of the copyright rules in France, in particular those resulting from Article 17 of the Copyright Directive and Articles L137-1 et seq. of the IPC;

(Recommendation 8) Specify, in the general conditions of use or in the online dispute forms, the possibility for users and rightholders to refer to Arcom's dispute settlement process, in the event of a dispute.

Rightholders could:

(Recommendation 9) Produce reference information on copyright and its exceptions so that it can be made available by providers of a content-sharing services;

(Recommendation 10) Systematically pursuit the conclusion of agreements, in particular with regard to rightholders in photography and publishing;

(Recommendation 11) Ensure that Arcom is provided with all the answers it needs to carry out its evaluations;

(Recommendation 12) inform Arcom of the agreements concluded.

Both parties could:

(Recommendation 13) Continue to collaborate with the goal of concluding agreements and open these agreements to all cultural sectors.

Scope and methodology

Definition of content-sharing service providers

Article L. 137-1 of the IPC defines an online content-sharing service provider as: "*the person who provides an online public communication service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which the service provider organises and promotes for profit-making purposes, either directly or indirectly*"[3].

This article explicitly excludes the following from this definition:
- Not-for-profit online encyclopaedias;
- Not-for-profit educational and scientific repositories;
- Open source software development and sharing platforms;
- Providers of electronic communications services as defined in the European Electronic Communications Code[4];
- Online marketplaces;
- Business-to-business cloud services;
- Cloud services that allow users to upload content for their own use;
- As well as illegal sites whose purpose is to infringe copyright and related rights, for which the specified provisions do not apply.

The national legislator has advised that "*the assessment of whether (...) gives access to a large amount of copyright-protected works and protected subject matter (...) should take account of the number of files of copyright-protected content uploaded by users of the service, the type of works uploaded and the audience of the service*"[5].

The order of 20 October 2021[6] specifies the audience threshold and the minimum number of files of content uploaded by users, according to the type of works concerned, that should be taken into account when assessing the "large amount" of works uploaded by users:
- The audience threshold is set at 400,000 unique visitors in France per month per online content-sharing service providers calculated according to the last calendar year;
- The thresholds for the number of files of content uploaded by users are as follows:

---

[3] This definition is used as a reference for related rights in Article L. 219-1 of the IPC.
[4] Namely services providing signal transmission services.
[5] French Decree no. 2021-1369 of 20 October 2021, implementing Article 1 of Decree no. 2021-1369 of 20 October 2021, Art. 1.
[6] Regulation of 20 October 2021, implementing Decree no. 2021-1369 of 20 October 2021, amending the Intellectual Property Code and relating to certain online content-sharing service providers.

Table 1: Thresholds by type of work

Type of work included in the content file	Number of content files
Audiovisual works	100
Radio works including podcasts	100
Musical works	5,000
Works of visual art	10,000
Written works, including press articles and audiobooks	100
Video games	100
Content including all types of works	10,000

Source: Regulation of 20 October 2021

Obligations for content-sharing service providers

By providing access to copyrighted works uploaded by their users, online content-sharing service providers perform an act of representation for which they must obtain prior authorisation from the rightholders[7].

Generally, the agreement authorising representation of the works will provide for remuneration for the rightholders, either by determining a lump sum payment or according to the principle of proportionate remuneration, associated with the actual use of each work belonging to the rightholder concerned.

In practice, content-sharing service providers therefore require technological tools to identify the works and how much those works are actually used, which explains why service providers use technological identification measures (TIMs).

In the absence of authorization and to avoid liability, content sharing service providers must[8]:

- Have made, in accordance with high industry standards of professional diligence, their best efforts to ensure the unavailability of specific works for which the rightholders have provided them with the relevant and necessary information, whether directly or indirectly through a third party. In this case, content-sharing service providers require technological tools to identify the works.

- Have in any event acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their service, the notified works, and made best efforts to prevent their future uploads. If rightholders fail to provide information allowing automatic tools to identify content when made available on the service, they must take subsequent action and be capable of informing service providers of any unauthorised use of their work.

---

[7] IPC, Art. L. 137-2, I.
[8] IPC, Art. L. 137-2, III.

![Arcom logo](The Regulatory Authority for Audiovisual and Digital Communication)

Assessment of technical measures for identifying protected works and objects implemented by online content sharing service providers

This mechanism can be represented as follow (Fig. 1). In practice, there is a partial overlap between the different technologies. Since an upload can only be blocked if the content has been identified, protection technologies also serve as content recognition technologies. In this report, they will generally be referred to as technological identification measures (TIMs).

Since the technological tools (fingerprinting, hashing, metadata or watermarking) can only be used to identify works, choices made by the rightholders determine which rules are applied (tracking, monetisation or blocking).

Figure 1: Diagram illustrating Article L. 137-2 of the IPC:

Source: Arcom
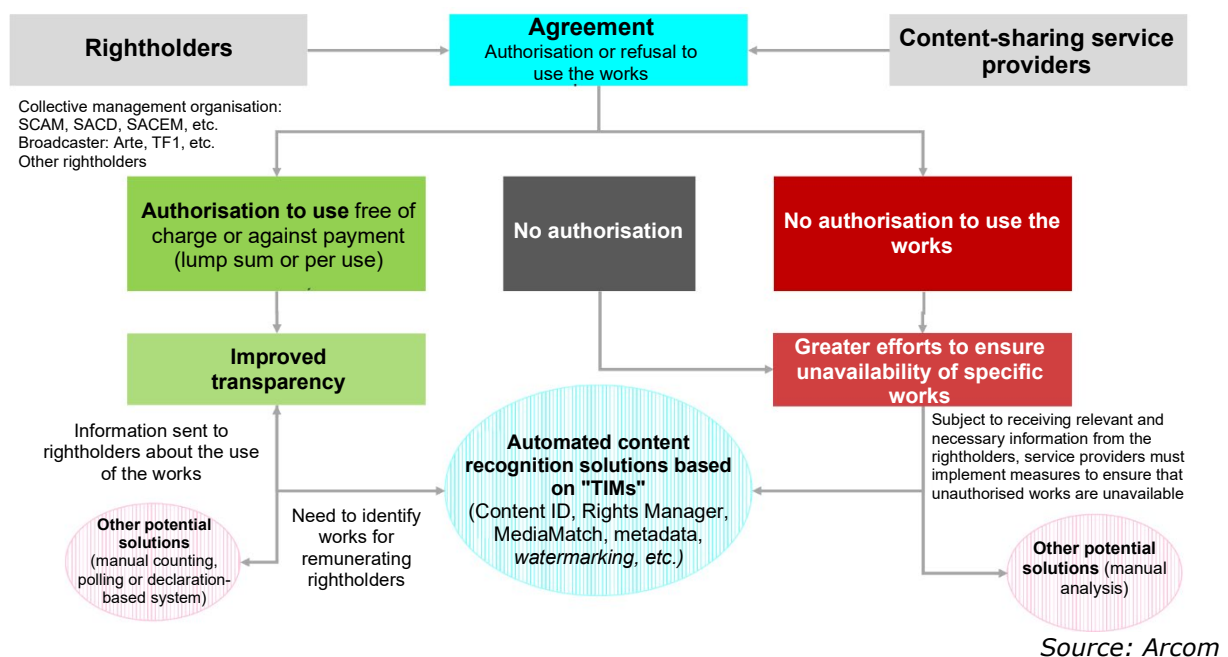
In addition, Article L. 137-2 of the IPC[9] specifies a reduced level of professional diligence for service providers that have been making their services available to the public within the European Union for less than three years <u>and</u> whose annual turnover is less than €10 million.

---

[9] IPC, Art. L. 137-2, 3°.

Table 2: Obligations for content-sharing service providers

Normal scheme	Simplified scheme: applicable to providers that have been making their services available to the public within the EU for less than three years and whose turnover is less than €10 million
Where no authorisation has been granted, the content-sharing service provider is <u>not liable if it demonstrates</u> that: - It has made its best efforts to obtain an authorisation - It acted expeditiously, upon receiving notice from the rightholders, to disable access to or remove the content - It has made, in accordance with high industry standards of professional diligence, its best efforts to ensure unavailability	**Where there are fewer than five million unique visitors a month**: The service provider must: - Make its best efforts to obtain an authorisation - Act expeditiously, upon receiving notice from the rightholders, to disable access to or remove the content **Where there are more than five million unique visitors a month**: In addition to the above obligations, the service provider must make best efforts to prevent further uploads of the notified works for which the rightholders have provided relevant and necessary information

Source: Arcom (Article L. 137-2 of the IPC)

Methodology

In its Recommendation 1, the High Authority for distributing works and protecting rights on the Internet (Hadopi, become Arcom in 2022 had identified 13 service providers that were likely to be subject to Articles L. 137-1 et seq. of the IPC[10]. They had been chosen according to their audiences, which were higher than the thresholds defined in the Regulation of 20 October 2021, and the amount of protected works and content made available to the public.

Table 3: Average monthly audience for the content-sharing service providers identified by Hadopi

Service providers	Category	Average monthly audience in 2021 (in thousands)
Dailymotion.com	Video content	7,631
Facebook	Various content	46,608
Instagram.com	Images (mainly)	20,679
LinkedIn	Various content	11,427
Pinterest.com	Images (mainly)	10,216
Reddit.com	Various content	1,441
Snapchat	Video content	23,842
Soundcloud.com	Audio content	704

---

[10] https://www.hadopi.fr/organisation/avis/recommandation-mesures-protection-oeuvres-et-objets-proteges-fournisseurs-services-partage-contenus-en-ligne.

Arcom
The Regulatory Authority for
Audiovisual and Digital Communication

Assessment of technical measures for identifying protected works
and objects implemented by online content sharing service
providers

Service providers	Category	Average monthly audience in 2021 (in thousands)
Tiktok.com	Video content	6,950
Twitch.tv	Video content	3,525
Twitter.com	Various content	9,401
Vimeo.com	Video content	1,249
YouTube	Video content	46,695

Note for the reader: Médiamétrie // Netratings audience data based on a panel of 30,000 individuals representative of the French population aged 2 and over (three-screen viewing).

Source: Arcom (Hadopi)

Taking into account the audience achieved, the means implemented by service providers to block or prevent content uploading, and the quantity of content blocked or removed, allowed for an estimation of the magnitude of protected content made available by the services in relation to the thresholds set in the order.

Based on this scope, Arcom launched a consultation process with the relevant stakeholders (online content-sharing service providers and rightholders) by publishing two questionnaires[11] on its website from 28 April to 13 July 2022.

The questionnaires were designed to ask service providers and rightholders about the protection measures implemented and especially the application of legal provisions, agreements to authorise or block content between service providers and rightholders, and the various tools and measures proposed by service providers for reporting works and ensuring their unavailability. The aim was also to specifically gather feedback from rightholders about the tools available.

The Authority made direct contact with the 13 service providers identified by Hadopi to invite them to complete the questionnaire that had been uploaded for their attention.
- **Seven of them took part in the consultation**, either fully or partially:
  o Dailymotion
  o LinkedIn
  o Meta (for its Facebook and Instagram services)
  o Pinterest
  o TikTok
  o Twitter[12]
  o YouTube
- **Five did not respond**:
  o Reddit
  o Snapchat
  o SoundCloud
  o Twitch
  o Vimeo

In addition to the data and information received from the service providers that replied to the consultation, publicly available information and data (transparency report, access to reporting forms, etc.) were also analysed.

---

[11] Available in the appendix.
[12] Twitter disputes its classification as a "content-sharing service provider", but since it replied to the consultation, the information provided has been included in this report.

In addition, Arcom received **50 responses** (complete or partial) from **50 rightholders**[13]**:**
- Eight from the publishing sector (publishers and unions)
- Ten from the audiovisual sector (producers, distributors and collective management organisations)
- Eleven from the music sector (publishers, producers, distributors and collective management organisations)
- Twenty from the photography sector (freelance photographers and collective management organisations)
- One from the "other" category (university)

This report is based on the respondents to the consultation, i.e. seven service providers and fifty rightholders.

Building on the work carried out in 2020 by the CSPLA (Higher Council for Literary and Artistic Property), Hadopi and the CNC (National Centre for Cinema and Moving Image), rightholders were asked to assess the protection measures against three criteria[14]: robustness, usability and selectivity (refer to the section entitled "Assessment into the technological identification measures" later in this report).

---

[13] The list of rightholders who completed the questionnaire is available in the appendix.
[14] Refer to the CSPLA, Hadopi and the CNC: "Steps towards effective copyright enforcement on digital sharing platforms: review and proposals for content recognition tools", January 2020 and Hadopi's Recommendation 1.

Report

Article L. 137-2 of the IPC states that "*by providing access to copyrighted works uploaded by their users, online content-sharing service provider perform an act of representation for which he must obtain prior authorisation from the rightholders, notwithstanding the authorisations that he must obtain under the right of reproduction for any reproductions of the said works*."

Where no authorisation has been granted, part III of that article sets out the three conditions that service provider must fulfil to avoid incurring their liability:

"*a) It made its best efforts to obtain an authorisation from the rightholders who wish to grant such authorisation*

(b) It made, in accordance with high industry standards of professional diligence, its best efforts to ensure the unavailability of specific works for which the rightholders have provided the service providers with the relevant and necessary information, whether directly or indirectly through a third party

(c) It has in any event acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from his service, the notified works, and made its best efforts to prevent their future uploads in accordance with point b"

This report is intended to shed light on rightholders' perceptions and degree of satisfaction concerning the effectiveness of the tools offered by service providers and their efforts to comply with the requirements of Article L. 137-2 of the IPC. This report will start by reviewing the content recognition tools made available by content-sharing service providers and how those tools are perceived by rightholders.

Removing and disabling access to content will be covered in the second part of this report for the purpose of assessing service providers' ability to act expeditiously upon receiving a notice from rightholders. This report will also examine whether reporting forms are easy to access and use, as well as their effectiveness.

Finally, the third part of this report will address the existence of agreements authorising the use of content or allowing access to recognition tools.

I.   Technological identification measures:

II.   perception and uses

Arcom asked content-sharing service providers whether they had developed tools to identify content and thereby prevent content protected by copyright or related rights from being made available on their services, and well as details on how their tools worked. When using such tools and providing relevant and necessary information, rightholders were asked to indicate how much they knew about these tools and how much they used them. Rightholders were also prompted to assess their usability.

Technological measures for identifying content

Existing technologies

The report published by the CSPLA, Hadopi and the CNC in 2020[15] identified four different identification technologies:
- Hashing
- Watermarking
- Metadata analysis
- Fingerprinting

Any of these technologies can be used to identify content made available by a content-sharing service.

Hashing

Hashing is a technology that represents a data item or computer file as a unique alphanumeric character string: "*the principle is to transform a data item or file (e.g. a password or an image, video or sound file - irrespective of its size) into a series of 32 to 128 characters*"[16].

By transforming a data item into a series of characters, the hash code becomes a unique signature. Each protected content, regardless of its type (image, sound or video), can be represented by a specific hash code that will identify the content when integrated and compared to a reference database. Hashing is a relatively fragile technology, since the slightest modification to the original hashed file will end up generating a different hash code to the first.

Watermarking

Watermarking, which is especially used for video, sound and images, involves "*embedding content with a specific signal that can subsequently be detected. A watermark is a type of signature incorporated into the work. The watermark can be detected with an appropriate tool and can be used to identify the original and any copies. Two instruments are required to implement this technology:*

---

[15] CSPLA, Hadopi, CNC, *op. cit.*
[16] *Ibid.*

- *A marker whose role is to watermark the content*
- *A detector whose role is to scan the content for any watermarks*[17]

Metadata

Metadata are data that define or describe other data, such as the date when content was created, the author of a photograph, the title of a work or the GPS location of the place where the image was taken.

"*Metadata can be embedded directly into the files containing the works, depending on their format (for example, metadata can be integrated into images and MP3 audio files). They can also be stored in a separate database, as long as an identifier is used to link each content with its metadata. By simply querying the database, and provided that this information has been entered, users can identify all the content that was created before a given date or find all the works created by the same author, or all the paintings whose title contains a specific word.*"[18].

Fingerprinting

Fingerprinting systems are based on generating and then using a unique digital representation of the content, regardless of its type, which constitutes a "fingerprint" of the content. The fingerprint is separate from the work that it identifies.

The 2020 report stated that "*fingerprinting systems establish (...) the similarity between two items of content by comparing their fingerprints. The technologies used to generate the fingerprints consist in reducing or simplifying the entire content (image, sound, video, text, etc.) and only retaining the characteristic elements. (...) Instead of directly assessing the similarity between two documents (two images, two soundtracks, two texts, etc.), these tools establish their similarity by comparing their fingerprints*[19]."

More specifically, a content recognition system "*comprises (...) a reference database containing the fingerprints of all documents to be identified. (...) Once this database has been created, the system is used as a search engine. When looking to check whether an unknown document exists in the reference database, its fingerprint is first extracted before comparing it with the pre-computed fingerprints stored in the database. This comparison can then determine whether similar documents have been found. (...) One or more matches can be established between the fingerprint of a document to be identified and the fingerprint of an unknown document. Above a certain similarity threshold, the two documents in question can be considered to be effectively similar*[20]."

Knowledge of the tools by rightholders

Just over half the respondents (52%) consider that they are well informed about the tools available for protecting, monetising and tracking the dissemination of their content.

Specifically, 15 respondents claimed that they had undertaken their own research to find out what tools were available from service providers. A minority (fewer than five respondents) advised that they do not look for information and consider that service providers are responsible for informing rightholders. In their opinion, service providers

---

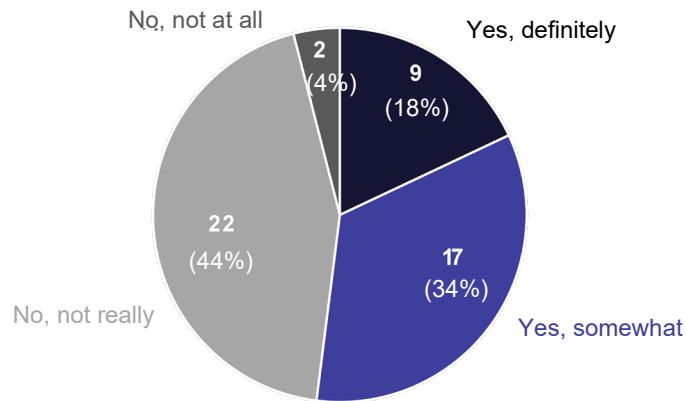[17] CSPLA, Hadopi, CNC, *op. cit.*
[18] *Ibid.*
[19] *Ibid.*
[20] *Ibid.*

should contact rightholders to explain how their tools work and inform them of any updates and the process for creating fingerprints.

Figure 2: Knowledge of the content identification tools

Base: all respondents (50 rightholders)

Source: Ifop study for Arcom, 2022

Audiovisual rightholders appear to be the best informed (seven of the ten respondents in the audiovisual sector claimed to be "well informed"). According to them, this good level of information can be attributed to the fact that anti-piracy measures are a key issue in the online distribution of their content, since audiovisual content has long been subject to widespread illicit practices. In addition, the initiatives spearheaded by the ALPA (Audiovisual Anti-Piracy Association created in 1985, of which some respondents are members) and the graduated response procedure implemented in 2009 have helped alert the sectors' stakeholders to the need to tackle piracy. Finally, their relationship with such service providers as YouTube, Facebook and Dailymotion has allowed them to embrace these technologies.

However, one rightholder spontaneously advised that there was no information about the tools to protect content over instant messaging services, which can be used to exchange various types of content, including videos, in discussion groups featuring up to several thousand people.

The situation for music rightholders is clear-cut, since half the respondents claim that they are well informed, while the other half is the complete opposite.

This good level of knowledge can be explained by the licensing agreements with service providers and their discussions with those service providers. One respondent stated that some service providers communicate with their partners and offer workshops, webinars or certification schemes. At the same time, in-house technical skills improve understanding of the tools available.

Conversely, the music rightholders who claim that they are ill-informed are those who have not signed an agreement with the service providers and do not seem to have the necessary in-house expertise to be fully proficient in using the tools.

Finally, rightholders in the book publishing and photography sectors generally feel that they are not well informed. Book publishers explain this situation by the lack of discussions

with service providers, while photographers point to a lack of communication from service providers about the tools available.

> Content-sharing service providers could:
>
> ➢ **Recommendation 1**: improve information towards rightholders of any sectors regarding recognition tools at their disposal;
>
> ➢ **Recommendation 2**: propose training courses or give access to tutorials to rightholders, even through collective management organisations, in order to help them to master recognition tools.

Tools used in different ways

Rightholders use these technologies in different ways. Their use depends on the performance of the solution and the type of content, as well as the rightholders' technical, financial and human resources, and more generally the extent of their knowledge about content protection solutions.

In all, 34 rightholders claimed that they use content recognition technology. Only two of them (from the music sector) use hashing.

Fifteen rightholders advised that they use watermarking, including six rightholders in the music sector, four in photography, three in audiovisual and two in publishing.

Seventeen rightholders reported using fingerprinting: eight in the audiovisual sector, seven in music, one in publishing and one in photography.

Finally, 25 rightholders claimed that they use metadata: nine in the photography sector, six in music, six in publishing and four in audiovisual. The over-representation of rightholders using metadata, especially compared to those using fingerprinting, can be attributed to the fact that this technology is widely used by photography rightholders, who were the largest group to answer the questionnaire.

Figure 3: Content recognition technologies used by rightholders
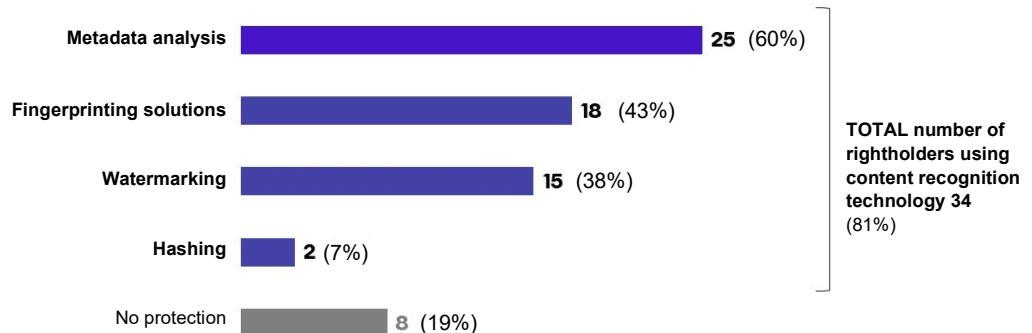
Base: 42 respondents to Q6. *With respect to the content that you (or your company) produce, distribute or broadcast, do you use technological solutions (fingerprinting, watermarking, metadata, etc.) to monetise or protect it against unauthorised reuse? [more than one answer possible]*

Source: Ifop study for Arcom, 2022

The study reveals that almost a fifth (19%) of the rightholders who answered this question during the consultation claimed that they do not use technological solutions to protect their works when communicated to the public and uploaded to the websites of online content-sharing service providers. This figure can be explained by the fact that these rightholders claim that they are poorly informed about the range of technological solutions available (see above) and they consider that the solutions available are not always suited to their needs.
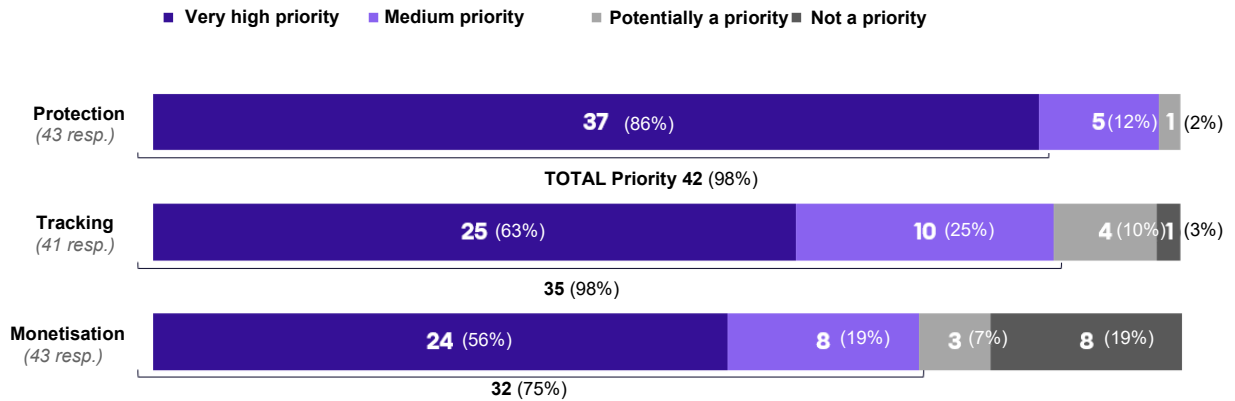
As for the seven service providers who participated in the consultation, only five indicated that they use one (fingerprinting) or more content recognition technologies, and one of them stated that it uses other tools based on different technologies but for other purposes (to protect its audience).

The tools are mainly used to protect content

Generally, rightholders in every sector consider that protecting the content disseminated over content-sharing services (i.e. blocking content in response to a copyright infringement) is a top priority (86%). Tracking viewership comes next on the list (63% consider this to be a very high priority), followed by monetisation (56%).

Note that the tools made available by service providers to identify content can therefore be used to track viewership as well as monetise or block content.

Arcom The Regulatory Authority for Audiovisual and Digital Communication

Assessment of technical measures for identifying protected works and objects implemented by online content sharing service providers

Figure 4: Priority level identified for the dissemination of content over content-sharing services

Legend: ■ Very high priority ■ Medium priority ■ Potentially a priority ■ Not a priority

Protection (43 resp.): 37 (86%) | 5 (12%) | 1 (2%) — TOTAL Priority 42 (98%)

Tracking (41 resp.): 25 (63%) | 10 (25%) | 4 (10%) | 1 (3%) — 35 (98%)

Monetisation (43 resp.): 24 (56%) | 8 (19%) | 3 (7%) | 8 (19%) — 32 (75%)

Base: 43 respondents claimed that they use the tools for protection and monetisation, and 41 for tracking viewership (answers to Q5). For you and your company, what priority level would you give to the dissemination of your content over content-sharing services?

Source: Ifop study for Arcom, 2022

Rightholders have access to different content management methods

The most common features offered by the tools include monetising and blocking content. Fingerprinting technologies generally offer these two options, as well as the possibility of tracking viewership, which is a prerequisite for monetisation.

When accessing the tool, rightholders whose content has been uploaded by a user without authorisation can request its removal using the options available for this purpose. The solution may specify the geographical range of the measure and apply it only to certain specified regions/countries. Rightholders may also decide to allow their content to be disseminated by monetising it.

With this aim in mind, rightholders have a CMS interface (content management system) on the service providers' websites for tracking the management of their content. Service providers' proprietary tools (*Content ID*, *Copyright Match Tool*, *MediaMatch*, *Content Claiming Portal* and *Rights Manager*) offer such an interface.

For example, Pinterest's "NoPin Code" feature allows rightholders to prevent users from uploading copyrighted content where the rightholders have already communicated such content to the service.

Pinterest also enables rightholders to be assigned with all the "pins" containing their content. Their content is not removed and is still accessible, but its right of attribution is restored.

The priority that rightholders give to the importance of protecting, tracking and monetising content varies from one cultural sector to the next.

Table 4: Degree of importance that rightholders attach to protecting, tracking and monetising their content

	Protection	Tracking	Monetisation
Audiovisual	***	**	*
Music	**	***	**
Publishing	***	**	*
Photography	***	**	*

*** very important / ** important / * not important

Source: Arcom based on a questionnaire

Assessment of the technological identification measures by rightholders

Rightholders were invited to assess the different technologies by assigning a score out of 10 to different items under three main criteria[21]: robustness, usability and selectivity.

The **robustness** of the protection measures refers to the tool's ability to effectively and automatically recognise protected content, even when the content has been altered. Rightholders had to answer questions about the technologies' detection capabilities for different types of content (sounds, still images, moving images, speech, live content, etc.), the detection time, the degree of coverage across all accounts on the service[22], the resilience to circumvention attempts (cropping, change of video speed, change of colour, etc.), the possibility of adapting different rules for different regions/countries, the option of defining specific rules for several rightholders for the same content, the effectiveness at identifying content, the tool's adaptability (to changes in infringement practices), and the period of protection.

Rightholders measure **usability** in terms of the tool's practicality during use. Rightholders were asked to comment on the tool's ease of use, its alignment with their specific needs, its wealth and variety of features, its learning curve, the transparency of its operating rules, its updates, the technical support service, relations with the content-sharing service provider for learning how to use the tool, the validity period for fingerprints, backward compatibility with old fingerprints or the reporting tools provided.

Finally, **selectivity** refers to the solution's ability to block infringing content only. Its analysis was based primarily on the data that service providers submitted about disputes against decisions to disable access.

Arcom regrets the low number and even lack of replies from rightholders on these particular points. As such, Arcom has very little data about certain technologies or specific uses. A larger amount of contributions would help better identify the tools or features that

---

[21] Refer to the questionnaire in the appendix, Q. 29 to Q. 30 for fingerprinting users and Q. 31 to Q. 33 for users of other technologies.
[22] In other words, the tool's ability to identify content across all the proposed accounts and services.

the Authority could specifically examine or assess in greater detail where difficulties or limitations are reported by a high number of respondents.

Hashing

Only two rightholders in the music industry claimed that they use the hashing technology, and only one of them scored the technology.

In terms of robustness, the rightholder gave a score of 10/10 for the technology's detection capabilities, the detection time and the resilience to circumvention attempts. The rightholder also gave a score of 5/10 for the degree of coverage, the effectiveness at identifying content, updates to the tool and its level of backward compatibility, i.e. its ability to identify works protected with earlier versions of the technology.

As for usability, the rightholder gave 10/10 for the tool's ease of use, alignment with specific needs and learning curve, and finally 3/10 for the wealth and variety of features.

Arcom regrets that it only received a few evaluations of this technology, which can be explained by the fact that it is not widely used and not the most suited to protecting content, particularly videos.

In addition, only one service provider indicated that it used hashing-based recognition technology, but other than for copyright protection purposes.

Watermarking

Five of the fifteen rightholders who advised that they use watermarking actually assessed it: two in the music sector, two in photography and one in audiovisual.

In terms of robustness, the audiovisual rightholder gave a score of 8/10 for the technology's degree of coverage across all services and the possibility of assigning specific rules for several rightholders. The two music rightholders have a different opinion of the tool. Although one is highly satisfied with the option of assigning specific rules (10/10), the other seems far less satisfied (5/10). Furthermore, although one is highly satisfied with the detection capabilities and degree of coverage (10/10), the other is very satisfied with updates to the tool (10/10) and the resilience to circumvention attempts (9/10). Finally, while one of the two photography rightholders only assessed the possibility of assigning specific rules and seems fairly satisfied (7/10), the other claims to be satisfied with updates to the tool (8/10), fairly satisfied with its effectiveness and the possibility of assigning specific rules (7/10), and not very satisfied with its resilience to circumvention attempts (4/10).

As far as usability is concerned, only three rightholders (two in the photography sector and one in the music sector) assessed this criterion. The music rightholder is highly satisfied with the tool's alignment with specific needs (10/10), but less satisfied with the wealth and variety of features (5/10). Finally, while one of the photography rightholders appears to be satisfied with the ease of use, learning curve and transparency of the operating rules (8/10), the other does not seem satisfied with the use of the technology (4/10).

Once again, Arcom regrets the low number of replies from rightholders to the questionnaire posted online.

Note that the 2020 report considered that the watermarking technology could be used alongside fingerprint-based content recognition systems despite its greater fragility[23]. The watermarking technology embeds a marker into the content for ensuring its identification. Fingerprinting and watermarking are two different techniques that can be combined to good effect. Using both technologies allows rightholders to broaden the range of protection for their content. For example, watermarking may be more practical for identifying protected content when live-streamed.

The way in which both technologies dovetail is reflected in the replies from the 15 rightholders who claim to use watermarking. Twelve of them seem to use watermarking alongside another technology (mainly fingerprinting), and only three use it on its own.

In light of its potential fragility[24] and in line with the 2020 report, Arcom wishes to reiterate that the watermarking technology can be useful, especially if used alongside another content recognition technology, although its effectiveness may be limited when used alone.

Metadata

Of the 25 rightholders who claimed to use metadata, only four assessed the technology (three in the photography sector and one in the music sector).

As for robustness, rightholders differ in their assessments. The music rightholder (who only assessed half the items) is satisfied with the metadata and especially with the detection capabilities, the frequency for checking and analysing uploaded content, and the degree of coverage across all services (10/10). The photography rightholders appear to be moderately satisfied with the technology's robustness, with one attributing a score of 7/10 to its detection capabilities and the possibility of assigning specific rules for each rightholder, while the other gave a score of 6/10 to the detection capabilities and the frequency for checking and analysing uploaded content.

In terms of usability, the music rightholder only assessed four out of eleven items, but was highly satisfied with the tool's ease of use, alignment with specific needs and learning curve (10/10). Photography rightholders also only evaluated a few items. Their replies reveal that they are satisfied with the tool's alignment with their needs (10/10, 8/10 and 7/10), the wealth and variety of features (10/10 and 8/10), the transparency of the operating rules (10/10 and 8/10) and finally updates to the tool (10/10, 7/10 and 6/10). However, rightholders are dissatisfied with the tool's learning curve (5/10, 7/10 and 5/10).

As with hashing and watermarking, Arcom regrets the lack of replies and incomplete answers from rightholders, given the number of rightholders who claim to use the technology.

Metadata can be particularly useful where other means of identification, such as hashing or watermarking, are unavailable or unsuitable for the content that needs protecting.

---

[23] CSPLA, Hadopi, CNC, *op. cit*.

[24] "*Tech-savvy users can successfully blur or erase digital markers, such as by combining several separately marked versions together (this is known as a collusion attack). There are specialised watermarking algorithms that are resistant to collusion attacks, but they are complex and expensive. On the other hand, an unmarked copy, i.e. it has been created before watermarking, cannot be recognised by the system. Therefore, marking cannot be used retroactively and only serves to protect new streams of marked content (and not the stock of unmarked copies already in circulation). However, some interested parties are worried about the large-scale use of watermarking, since they fear that the technology's robustness could be undermined if too many parties have access to the watermark detection module. Malicious individuals could use reverse engineering in an attempt to reveal detailed information about how the system works, thereby weakening it,*" CSPLA, Hadopi, CNC, *ibid*.

Metadata can be used to determine the title or source of an image and identify the people or organisations who should be contacted to obtain a licence. They can advise whether or not a protected work is allowed to be uploaded to a content-sharing service.

The metadata technology is mainly used by photography rightholders (nine out of the twenty-five rightholders who claimed that they use metadata are from the photography industry), but it can be unreliable as emphasised in the 2020 report, especially due to the risks of mistaken identity[25] or the habit of some service providers to "*remove all or part of the metadata from the image files hosted. Although the volume of metadata is fairly insignificant for a feature-length video, it is anything but negligible for a thumbnail photograph (500 characters of uncompressed metadata can amount to 10 or 20% of the total weight of an image as a compressed thumbnail)*[26]".

Arcom's observations about removing metadata from images during uploads

Arcom carried out an initial series of tests in 2022 to update its knowledge about the practices used by the main content-sharing service providers for retaining, modifying and deleting image metadata. Most of its findings were made with a simple web browser and a desktop computer. Arcom's employees created an image that was subsequently enriched with a number of metadata, including test values. The image was then uploaded to Facebook, Instagram, Pinterest, TikTok and Twitter, and then recovered after sharing online. At the end of the test, the start and end fields were compared.

Arcom observed that some services, such as Facebook or Pinterest, only retain a limited selection of metadata, i.e. the author's name or copyright statement. Furthermore, Pinterest only retains metadata in IPTC format: if the author's name is given in EXIF or XMP format, it is deleted. Other services, such as Twitter, remove most metadata, including copyright information, and only retain technical data, such as the ICC colour profile (International Color Consortium) of the image. TikTok converts the image into a 10-second video, and when the video is recovered, the original metadata no longer appear.

Instagram is something of a special case, since the image cannot easily be recovered with a web browser. It is impossible to download the image with a right-click, and the interface does not offer a dedicated button, meaning that there is no other choice than to use a hyperlink pointing to the publication to (re)share it. This limitation is probably intended to preserve the source of the image for subsequently reposting the image, so that it remains linked to Meta's ecosystem. However, this practice could be counterproductive, since it may encourage users wishing to save an image to take screenshots in which all the metadata will be lost. In addition, it has been found that an image recovered from the HTML code of the Instagram page no longer contains the original metadata.

Although content-sharing services rarely retain the metadata of the image files, they often display certain publication-related information next to the image, such as the date and name of the user who posted the image on the service. Sometimes, they allow the user

---

[25] "*In particular, special care must be taken with the risk of same names. The name Pierre Richard may correspond to the screenwriter of the film "I Don't Know Much, But I'll Say Everything" and to the author of the book "The Trial of the League of Patriots", but in one case it is the name of the popular actor and in the other case it is the name of the Deputy of the Seine department between 1893 and 1903. Similarly, the title "Lord of the Rings" may* refer to the high-fantasy novels published in the mid-20th century, the trilogy of films released in the 2000s and the television series screened in 2022. Therefore, identifying content using metadata alone requires a degree of caution and generally a manual check or multiple cross-checks," CSPLA, Hadopi, CNC, *op. cit.*
[26] *Ibid*.

to add a description or context labels that help identify objects in the image, such as places, people or even the work if the user makes the effort to credit the author.

Facebook applies an image processing algorithm to each upload and gives each image a brief text description, which can be accessed using screen reading software for the visually impaired. Therefore, these metadata are actually "external metadata" relating to the images that are shared and generated by the actual service and not by the rightholder or user.

Finally, it was found that some services do not treat metadata in the same way, depending on whether an image is displayed at full size (or full screen) or as a reduced size preview. Therefore, the metadata seen on the same service will not necessarily have the same degree of completeness depending on the method used to recover the image.

While removing certain metadata from image files may be understandable for the purpose of protecting personal information, such as for users who are not aware that their photographs include their geolocation, or for reducing the weight of preview files when there is a high volume of metadata, the Authority notes that the consistent and complete deletion of such metadata, as practised by certain service providers, raises a number of question marks, especially when that information relates exclusively to the ownership of the rights and its deletion makes it harder or even impossible to identify the author of the work.

Figure 5: Example of removing metadata on Twitter

Sample image.jpg Properties			
General	Security	Details	Previous Versions

Property	Value
Description	
Title	My title
Subject	My subject
Rating	★★★★★
Tags	My tag
Comments	My comment
Origin	
Authors	My author
Date taken	01/01/2022 12:00
Program name	My program
Date acquired	01/01/2022 12:00
Copyright	(c) Author 2022
Image	
Image ID	My unique ID
Dimensions	2208 x 2208

Sample image_twitter.jpg Properties			
General	Security	Details	Previous Versions

Property	Value
Description	
Title	
Subject	
Rating	☆☆☆☆☆
Tags	
Comments	
Origin	
Authors	
Date taken	
Program name	
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	2208 x 2208

Source: Arcom

Fingerprints

Existing fingerprinting technologies and eligibility conditions

Seven different fingerprinting tools or technologies were identified for this first report:
- *Audible Magic*
- *Content ID*
- *Copyright Match Tool*
- *INA signature*
- *MediaMatch*
- *Content Claiming Portal*
- *Rights Manager*

Five of these seven tools and technologies are proprietary solutions, i.e. developed by the actual service providers, while the other two *(Audible Magic* and *INA signature)* are so-called "third-party" technologies, meaning that they have been independently developed by companies or organisations with no links to the service providers.

Eligibility for these tools is often subject to fulfilling the conditions defined by the platform, such as being a rightholder, having a significant amount of content online and a large audience, and possessing the necessary technical skills and knowledge to use the solution. In addition, some service providers reserve privileged access to their tool for rightholders with whom they have entered into an agreement.

For example, to access Meta's *Rights Manager*, rightholders must complete an online application form, which will be submitted to the service for approval according to the

The Regulatory Authority for Audiovisual and Digital Communication

Assessment of technical measures for identifying protected works and objects implemented by online content sharing service providers

following eligibility criteria: holders must own exclusive rights to their content, they must have a catalogue of content that they want to protect, and finally they must not have posted any content in the past that was removed for copyright infringement.

On the other hand, YouTube offers two tools. The first (*Content ID*) is reserved for partners who can prove that they have the "*necessary capacity and knowledge to use the tool responsibly*". Furthermore, the service specifies that it must be able to "*determine whether* [rightholders] *really need Content ID and whether their content can be claimed through Content ID. Copyright owners also have to give evidence of the copyrighted content for which they control exclusive rights*[27]." The website also adds that "*if a copyright owner is approved for Content ID, they'll have to complete an agreement. This agreement will explicitly state that only content with exclusive rights can be used for reference. Also, they'll need to give the geographic locations of exclusive ownership, if not worldwide*[28]".

The second (*Copyright Match Tool*) is available to some YouTube users to prevent their content from being reposted by other users[29]. The tool is available to users who have previously submitted a valid copyright removal request. Subsequently, the tool starts scanning YouTube uploads for potential matches to the videos reported in the removal request, but with much more limited features than *Content ID*.

Finally, Pinterest and TikTok restrict access to their tools to anyone owning copyright to content[30].

In practice, the use of content recognition tools is subject to signing a user agreement and accepting the tool's terms of use. Therefore, there is no way that rightholders can use a solution like *Content ID*, *Rights Manager* or *MediaMatch* without authorisation from the service providers or at least without accepting the terms of service.

Table 5: Existing fingerprinting technologies and eligibility conditions

Tools	Service providers	Eligibility criteria
Audible Magic	Dailymotion (non-proprietary)	Own the copyright
Content ID	YouTube (proprietary)	Reserved for partners who can prove that they have the "*necessary capacity and knowledge to use the tool responsibly*" or for owners working with third-party service providers. Copyright owners must have the exclusive rights to the material evaluated.
Copyright Match Tool	YouTube (proprietary)	Available to content creators
INA signature	Dailymotion (non-proprietary)	Not known
MediaMatch	TikTok (proprietary)	Own the copyright
Content Claiming Portal	Pinterest (proprietary)	Own the copyright
Rights Manager	Meta (proprietary)	Three main criteria:

---

[27] https://support.google.com/youtube/answer/1311402.
[28] *Ibid.*
[29] YouTube states that the *Content ID* detection technology also powers the *Copyright Match Tool*.
[30] https://help.pinterest.com/en-gb/article/get-started-with-the-content-claiming-portal.

Tools	Service providers	Eligibility criteria
		- Content eligibility (own exclusive rights to the content) - Content catalogue (number of pieces of content to be protected) - Past infringements or violations (content removed in the past for copyright infringement)

Source: Arcom

However, it should be pointed out that legislation does not specify any particular conditions that rightholders must meet to qualify for the measures implemented by content-sharing service providers for protecting works and other subject matter.

Therefore, it would be desirable for service providers to offer solutions or tools to all rightholders and adapt those tools to rightholders' profiles like YouTube with its *Copyright Match Tool*, which has been developed for rightholders without access to *Content ID*.

> Content-sharing service providers could:
>
> ➢ **Recommendation 3**: set up simplified tools for rightholders who do not have the technical and economic resources to use complex tools;

Robustness assessment

In all, nine rightholders (five in the audiovisual sector and four in the music sector) assessed their use of the *Content ID*, *INA signature* and *Rights Manager* solutions.

Seven rightholders assessed their use of *Content ID* (four in the audiovisual sector and three in the music sector).

Audiovisual rightholders tend to be highly satisfied with the tool. Their satisfaction can especially be attributed to the frequency for checking and analysing uploaded content (with an average of 8/10), the degree of coverage across the whole service, the possibility of assigning specific rules for each rightholder, the period of protection and the effectiveness at identifying and recognising content (9/10 for each item), although two respondents consider that the technology *"still has limitations when it comes to detecting works"*. Rightholders are less satisfied with updates to the tool (6.8/10). In addition, one rightholder seems to be unhappy with the frequency for checking and analysing uploaded content (4/10).

As for the three music rightholders, only two assessed most of the items, while the third only scored the tool's resilience to circumvention attempts (cropping uploaded content and changing colours to circumvent protection measures) (9/10) and its effectiveness (9/10). The other two are satisfied with the detection time, the possibility of adapting specific rules according to the region/country (9.5/10 for both items) and the effectiveness at identifying and recognising content (8.3/10). The reason for dissatisfaction tends to concern the degree of coverage across the whole service (5.5/10).

Overall, the seven rightholders who assessed *Content ID* are highly satisfied with the solution's robustness, especially the duration of its protection measures and its effectiveness at identifying and recognising content.

![Arcom logo]

Assessment of technical measures for identifying protected works and objects implemented by online content sharing service providers

The *INA signature* tool was only assessed by two rightholders in the audiovisual sector. One was very satisfied with the solution (average score of 8/10) while the other was far from happy (average score of 3/10).

Given the very low number of evaluations (two) and their diametrically opposed opinions, it is hard for Arcom to reach an objective assessment about the tool. The Authority regrets that the five rightholders who claimed to use the INA signature solution did not assess its performance.

Finally, *Rights Manager* was assessed by five rightholders from the audiovisual sector and two from the music sector.

The audiovisual rightholders are satisfied with the degree of coverage across the entire service (7.7/10) and the period of protection (7.3/10), but less happy with the frequency for checking and analysing uploaded content (5/10), with one respondent even stating that "*Rights Manager takes quite a long time to analyse the stock*". On this particular point, some service providers have advised that they are unable to analyse the entire stream of incoming content, but tend to focus on content that has attracted a significant audience or been uploaded by a channel with a large number of subscribers.

As for the two music rightholders, one gave an overall assessment of the tool, while the other only evaluated the degree of coverage across all the accounts on the platform and the effectiveness at identifying and recognising content (7/10). The first music rightholder is particularly satisfied with the detection time, the possibility of adapting different rules for different regions/countries and establishing specific rules for several rightholders (10/10), but less happy with the frequency for checking and analysing uploaded content (4/10) and its resilience to circumvention attempts (5/10).

As for all the solutions, one rightholder claimed to be "*more or less satisfied with the measures implemented (...) to identify and protect content*".

In addition, the data received from the service providers helped reveal that the tools offer varying content detection times, ranging from a few seconds to several minutes after content has been uploaded to the services[31].

Table 6: Fingerprinting technologies and performance levels stated by the service providers

Tools	Stated performance level
Audible Magic	5-10 min
Content ID	Maximum of 2 min
Copyright Match Tool	Not known
INA signature	5-10 min
MediaMatch	A few seconds
Content Claiming Portal	Not known
Rights Manager	A few seconds

Source: Replies to Q21 of the questionnaire for content-sharing service providers: For each technology that you have deployed, please provide an accurate description of its technical operation

---

[31] The detection times for *Copyright Match Tool* and Pinterest's *Content Claiming Portal* are not available.

Usability assessment

Seven rightholders assessed the usability of the *Audible Magic*, *Content ID*, *INA signature* and *Rights Manager* tools. Five of those rightholders are from the audiovisual sector, while the other two are from the music sector.

The *Audible Magic* tool for recognising audio files was only assessed by two music rightholders. One of them only scored a single item (9/10 for backward compatibility and ease in creating fingerprints). The second rightholder appears to be generally satisfied with the solution and especially the reporting tool provided and the ease in creating fingerprints.

Once again, Arcom wishes to draw attention to the lack of replies to the questions about the tool's evaluation, which may limit the scope and exhaustiveness of the analysis.

Six rightholders assessed *Content ID* (four in the audiovisual sector and two in the music sector):
- audiovisual rightholders are very satisfied with the solution's ease of use and especially its alignment with their needs, the wealth and variety of features, backward compatibility with old fingerprints, the ease in creating fingerprints (8.5/10 for each of the items mentioned) and the validity period for fingerprints (9/10). The lowest-scoring item is the learning curve, which averaged 7/10 (still a satisfactory score).
- Music rightholders appreciate the wealth and variety of features and the validity period for fingerprints (8.5/10) as well as the ease in creating fingerprints (9.5/10). The points that could be improved include the tool's alignment with their needs (5/10), the transparency of its operating rules and updates to the tool (6/10).

As far as *INA signature* is concerned, three rightholders from the audiovisual sector assessed its usability. Nevertheless, due to the limited amount of data provided and their characteristics, Arcom is unable to properly assess the tool, since the rightholders did not complete all the items or had contrasting opinions about the solution. For example, one rightholder gave an average score of 8/10, while another gave an average score of 3.5/10 (no response from the third on this particular point).

Finally, seven rightholders assessed *Content ID* (five in the audiovisual sector and two in the music sector):
- four of the audiovisual rightholders provided an overall assessment of the solution, with the other only completed one item. Nevertheless, their feedback shows that their satisfaction with *Rights Manager* concerns the validity period of the fingerprints (8/10) and its ease of use (7.8/10), while reasons for dissatisfaction include the wealth and variety of features (5.6/10) and updates to the tool (5.3/10).
- Music rightholders are particularly satisfied with the validity period of the fingerprints (8.5/10) and the ease in creating fingerprints (9/10), but much less happy with its ease of use, alignment with their needs and learning curve (4.5/10).

Generally and with regard to the aspects causing dissatisfaction, rightholders stressed the lack of transparency from service providers on how their tools work, as well as the remuneration system, which some consider insufficient. In their words, there is a "*total lack of visibility and information about how the system works, the remuneration scheme, who can use what (...) without giving authorisation*".

The process of creating a fingerprint varies from one solution to the next

When creating a fingerprint, rightholders provide content-sharing service providers with relevant and necessary information, including information about the rights associated with the content (identification of the rightholders and geographical scope of use) and the blocking instructions written into the CMS.

There are two main options for creating fingerprints:
- Fingerprints are created using the CMS built into the technology offered by the content-sharing service provider or used by the service provider, the rightholder or a dedicated provider. Five rightholders in the audiovisual sector claimed that they create their own fingerprints directly on the platform, while two use a provider to generate the fingerprints.
- Fingerprints are created by the rightholder "in-house" without using the service provider's system, and the fingerprints are then sent to the service provider. Three rightholders use this process.

French anti-piracy association ALPA provides its members with a one-stop shop for creating fingerprints to protect their works on such platforms as YouTube and Facebook[32]. This one-stop shop aims to centralise the process of depositing works, creating fingerprints and dealing with conflicts[33]. To be eligible for this service, rightholders must be a member of ALPA, must be a producer or delegated producer of the work, and must have an ISAN number[34] for the work to be protected[35]. Only one rightholder claimed to use this system for creating fingerprints.

As for rightholders in the music sector, three create fingerprints on both the platforms and through a provider, and only one claimed to create fingerprints both in-house and through a collective management organisation.

The process of creating a fingerprint is relatively straightforward and similar for each of the tools offered by the service providers. Rightholders must send the platform or provider a file containing the work to be protected or its fingerprint (if already created) to populate the tool's reference database, which will help flag any matches with content subsequently uploaded by users. Rightholders also need to define what action must be taken if a match is detected (block or monetise).

Nevertheless, rightholders singled out the differences in how service providers support them with creating fingerprints or using the CMS to determine the various types of action required (track, monetise or block).

In practice, rightholders, collective management organisations, trade unions, associations and external service providers can create fingerprints. Generally, they are generated directly on the platforms, such as for Meta and YouTube with *Rights Manager* and *Content ID* respectively.

---

[32] An agreement was reached to this effect between ALPA and Google on 19 September 2017 and with Facebook on 26 July 2021.
[33] https://www.cnc.fr/documents/36995/144610/Guichet+unique+Protection+des+%C5%93uvres+audiovisuelles+sur+les+plateformes.pdf/6fe821dc-206f-0067-930e-bef11a4ceb95.
[34] The ISAN number (International Standard Audiovisual Number) is a unique, internationally recognised and permanent reference number for all kinds of audiovisual works (cinema, television, multimedia, video games, etc.), and can be compared to the ISBN number for books.
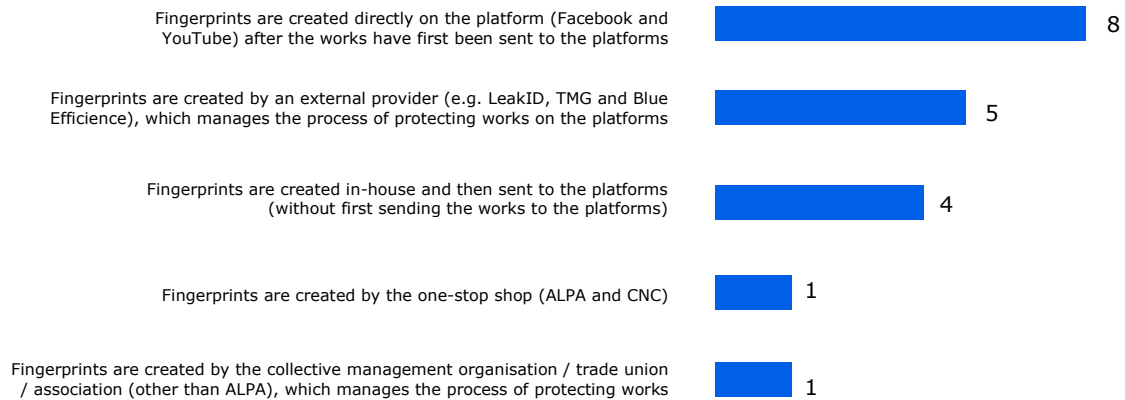[35] https://www.cnc.fr/documents/36995/144610/Guichet+unique+Protection+des+%C5%93uvres+audiovisuelles+sur+les+plateformes.pdf/6fe821dc-206f-0067-930e-bef11a4ceb95.

Conversely, the INA signature tool developed by INA (French National Audiovisual Institute) works in a different way. It is available to rightholders, who have direct access to the solution for generating the fingerprint for their content themselves, which is then integrated into a reference database. This solution (which can also be used by service providers) will then compare the content uploaded by the user service with its own reference database.

Figure 6: Creating fingerprints

|	
Fingerprints are created directly on the platform (Facebook and YouTube) after the works have first been sent to the platforms	8
Fingerprints are created by an external provider (e.g. LeakID, TMG and Blue Efficience), which manages the process of protecting works on the platforms	5
Fingerprints are created in-house and then sent to the platforms (without first sending the works to the platforms)	4
Fingerprints are created by the one-stop shop (ALPA and CNC)	1
Fingerprints are created by the collective management organisation / trade union / association (other than ALPA), which manages the process of protecting works	1

Base: 14 respondents claimed that they use fingerprinting solutions in response to Q22. If you use a fingerprinting solution such as Rights Manager, Content ID, Audible Magic or INA signature: who creates the fingerprints?
Source: Ifop study for Arcom, 2022

Not all rightholders have dedicated employees for creating fingerprints

The number of full-time employees for creating fingerprints or generally managing the technological identification measures varies according to the cultural sector and the size of the organisation.

Of the twenty-one rightholders who answered the question on dedicated human resources for implementing protection measures and managing the relationship with the content-sharing services, eight (five rightholders in the audiovisual sector and three in the music sector) advised that they had such measures, while thirteen did not. Large audiovisual and music groups are mainly the rightholders with specific human resources for these issues.

Figure 7: Dedicated employees for implementing technological identification measures

Yes — 8   No — 13
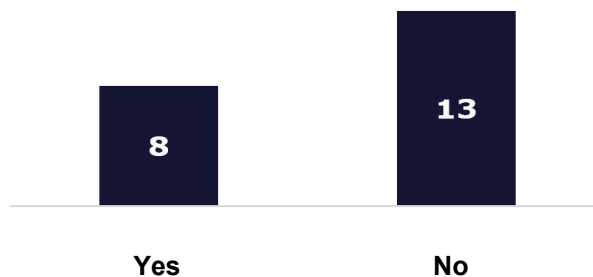
Base: 21 rightholders answered Q20. Does your company have human resources who are exclusively responsible for implementing measures to protect your content and managing the relationship with content-sharing services?
Source: Ifop study for Arcom, 2022

Rightholders are rarely informed of updates to the solutions and must constantly learn how to use them by themselves

Service providers regularly update their tools and are even continually developing their solutions. This may lead to both criticisms and satisfaction among the rightholders polled.

Adapting the tools is vitally important, given that users can be especially creative when it comes to circumventing disabled access and preventing protected content from being identified. However, constantly changing how the tools work can be a major headache for rightholders, who need to constantly learn how to use the solutions by themselves and understand the new detection rules. Rightholders are unhappy that service providers rarely offer training sessions on how to use their solutions or organise sessions to present the updates. They claim that discussions with service providers on using their tools are infrequent or non-existent. Undoubtedly, this explains the scores that the rightholders gave in their assessment into the usability of the different tools.

It appears that several rightholders can protect the same content on YouTube using *Content ID*. In this case, rightholders complained that YouTube lacked transparency when it came to determining which account has rights to the content concerned. Conversely, YouTube may also struggle to disable access when there are doubts about who owns the content.

Rightholders are rarely proficient in the technical skills required to use the tools

The difficulty that rightholders reported in getting to grips with the tools may have a dissuasive effect.

Rightholders are rarely proficient in the technical skills required to use the tools. The large audiovisual and music groups, which often claim to have dedicated employees for using the tools, run into fewer difficulties. However, even though they find it easier to get to grips with the solution, the process is still time-consuming and rarely suited to their needs.

Furthermore, the ease in receiving technical support depends on the service provider. Some rightholders advised that it could be hard to track down the relevant contact for resolving the problem or that service providers could be slow to respond and not always deliver the right answer.

Not all rightholders are convinced by the fingerprinting technology

Few rightholders shared information about their use of technologies other than fingerprinting.

Even though content-sharing service providers use the fingerprinting technology, it seems that this technology is not suited to every type of content, especially for photography and publishing rightholders. As far as rightholders in the publishing industry are concerned, the fact that current tools and technologies are not aligned with their needs explains one of the reasons why very few of them use identification technologies. Respondents indicated that more general information about the solutions available, technical training to learn how to use them and the development of user-friendly tools could convince them to use recognition technologies.

> Content-sharing service providers could:
>
> ➢ **Recommendation 4**: make content management systems (CMS) easier to use and supplement the management options offered.

Selectivity assessment

The last criterion, selectivity, refers to the ability to block infringing content only. However, this criterion could only be assessed using the figures published, where applicable, by the rightholders and service providers relating to disputes (or counter-notifications) brought by users who believe that they are in the right for uploading the content.

Selectivity is assessed according to the solution's ability to distinguish between content that has been made available for legitimate uses and pre-existing works (especially in relation to copyright exceptions) to avoid unduly removing or disabling access to content.

Article L. 137-4 of the IPC stipulates that the measures taken by service providers and rightholders must not deprive users of online content-sharing service providers of the effective benefit of the copyright exceptions provided for by the code. Therefore, online content-sharing service providers must put in place a complaint and redress mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of, works uploaded by them. Complaints submitted under the mechanism must be processed by the online content-sharing service provider in an expeditious and effective manner without undue delay.

In the event of a dispute about the follow-up action taken by the service provider in response to the user's complaint, the user may refer the matter to Arcom.
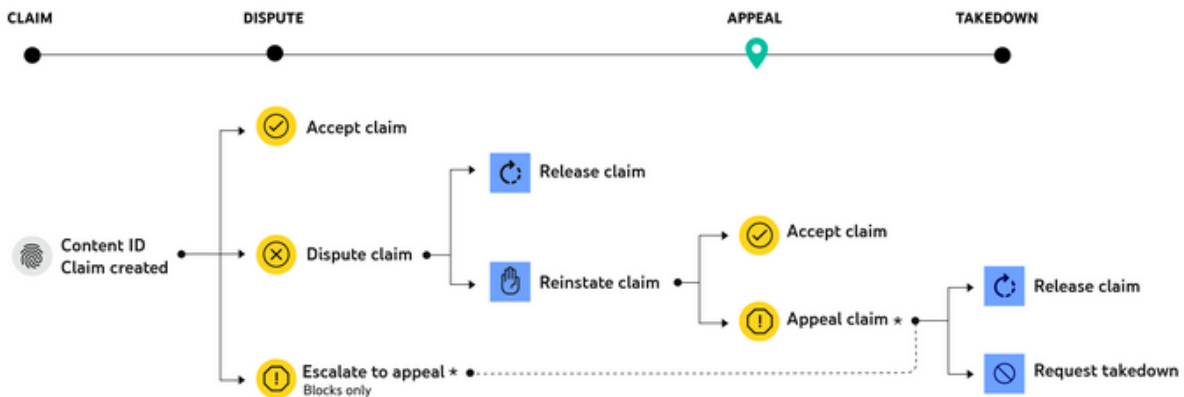
Tools still not very effective in detecting exceptions

The finding made in the 2020 report about the difficulties for recognition tools to identify parodies and pastiches[36] still seems to hold true. In this respect, Meta acknowledges in its response to the questionnaire that the tools are often unable to identify the context of the uploaded content, particularly if it contains a parody or other legitimate form of expression.

Users are then informed of the decision to disable access to, or remove, the content as well as the part of the content concerned. They are also notified that they can submit an appeal (or file a "counter-notification") against the decision by claiming an exception, including a quotation, criticism, review, caricature, parody or pastiche.

---

[36] CSPLA, Hadopi, CNC, *op. cit.*

![Arcom logo] **Arcom** — The Regulatory Authority for Audiovisual and Digital Communication

Assessment of technical measures for identifying protected works and objects implemented by online content sharing service providers

Figure 8: *Content ID* dispute and appeal process

Source: Appeal a Content ID claim, Help Center, Google.com

Action will only be taken for valid disputes

Users submit their dispute in the form of a "notification" (service providers have set up specific forms). Disputes must be considered valid by the service providers before any further action can be taken. The dispute must contain all the necessary information to identify the applicant (surname, first name, postal address and email address) and the content (date and time at which the content was blocked or reported, description of the content, URL link and justification and/or reason why the user believes that he/she is in the right).

Disputes are handled manually, and the processing time stated by the service providers varies between one and two days.

Service providers advise that the main reason for not approving or resolving notices or counter-notifications is when users submit incomplete forms. On this particular point, Dailymotion specifies that requests cannot be processed when users who have uploaded the blocked content refuse to present the necessary documents to substantiate their request or when users do not have legitimate information that could justify putting the content back online.

Rightholders in the audiovisual and music sectors indicate that they are familiar with copyright exceptions and that they pay special attention to any claims subject to an exception by evaluating them on a case-by-case basis.

It would appear that some disputes are unfounded and that users misconstrue or are unaware of the rules.

Although audiovisual rightholders are satisfied with how service providers handle disputes, music rightholders are less enthusiastic, some of whom complain about the lack of information when it comes to tracking and identifying the content removed.

Major audiovisual groups may need to address between 10 and 200 disputes every month from users whose content has been blocked or demonetised. The number of disputes received varies according to the service provider and fluctuates from one month to the

next. These numbers are much higher in the music sector, with one respondent claiming to receive over 1,000 disputes every day and per service provider[37].

Figure 9: Main reason for disputes
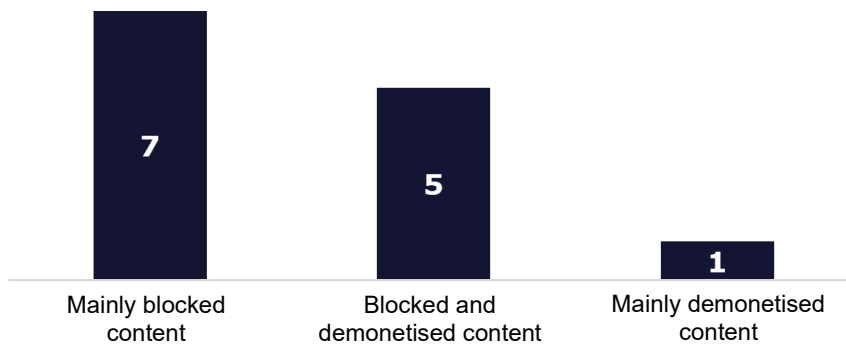
Base: 13 rightholders answered Q37. What is the main purpose for disputes, according to the content-sharing services: is the dispute related to blocked or demonetised content?

Source: Ifop study for Arcom, 2022

What happens to the disputed content depends on the service provider. In the event of a valid counter-notification, some service providers keep the content online until such time as the dispute has been settled, while others will block or delete it immediately, or vary between blocking and keeping it online depending on the dispute and appeal procedure, or even depending on the rightholders concerned.

Rightholders and users can keep track of the dispute on the service provider's website, or they receive a notification or email about the procedure's status.

The number of legitimate disputes subject to a copyright exception represents a tiny proportion of the content uploaded

The content recognition tools implemented by content-sharing service providers or running on their platforms are not sophisticated enough to detect and authorise uploaded content subject to a copyright exception.

However, feedback from service providers and rightholders suggests that the number of disputes subject to a copyright exception only represents a tiny share of the content uploaded. According to rightholders, these disputes are often ineligible for the claimed exception.

Number of notifications received worldwide in 2021 and processed by service providers

The transparency reports published by the service providers who took part in the consultation offer an overview of how they enforce copyright as well as information on their notices, disputes and counter-notifications.

---

[37] By way of example, music rightholders can submit a request to block content if an album is uploaded before its release date or if they wish to enforce their moral rights, such as if their content is being used for political purposes.

![Arcom logo](The Regulatory Authority for Audiovisual and Digital Communication)

Assessment of technical measures for identifying protected works and objects implemented by online content sharing service providers

However, it should be pointed out that the data available sometimes vary from one report to the next, meaning that there is no way to draw any satisfactory comparisons. The figures below, which are taken from the public reports released in 2021, are therefore provided for illustrative purposes.

- **LinkedIn**[38] received approximately 2,600 copyright infringement notifications. In 99% of the cases reported, the flagged content was removed.

- **Meta**[39] removed 33.8 million items of content from its Facebook service and 13 million from its Instagram platform by itself, i.e. before it received a notice from a rightholder, by using the *Rights Manager* tool alone. That same year, Meta received 1.6 million notices for Facebook and just over 700,000 for Instagram. Reported infringements of intellectual property rights resulted in the content being removed in about 85% of cases. This represents 5.8 million additional items of content for Facebook and 3.4 million for Instagram.

- **Pinterest**[40] received 47,633 notices during the second half of 2021. Only 28,655 of those notices were considered to be valid and were therefore processed. These takedown requests resulted in the deactivation of 148,778 pins (corresponding to 52,230 separate images).

- **TikTok**[41] received approximately 128,000 notices for intellectual property infringements. In 50% of cases, these notices resulted in the removal of the notified content.

- **Twitter**[42] received 318,653 takedown requests in 2021 for the Twitter platform, as well as 10,789 requests for Periscope and none for Vine. According to the service provider, the compliance rate for these requests was 31.3% for Twitter and 75.4% for Periscope. The amount of media withheld and therefore blocked as a result of the takedown requests was 1,938,639 for Twitter and 9,123 for Periscope. The number of tweets removed in 2021 was 594,742.

- **YouTube**[43] identified 1.48 billion items of content in 2021 with its *Content ID* technology. Of this content, 7.5 million (0.5%) items were disputed by users. YouTube took down 82,032 videos in response to the disputes, and subsequently there were approximately 4,500 counter-notifications, i.e. approximately 9% of the videos removed. Less than 1% of counter-notifications resulted in legal action. Furthermore, out of all the notices submitted by rightholders during the second half of 2021, YouTube estimates that 0.2% of the notified content was unfairly flagged, since it qualified as a copyright exception.

---

[38] Note that LinkedIn does not use or provide any content recognition tools or technology, LinkedIn, *Copyright removal requests*:
https://about.linkedin.com/transparency/community-report#copyright-removal-requests
[39] Meta, *Transparency Center, Notice and takedown*, 2021, H1 and H2:
https://transparency.fb.com/data/intellectual-property/.
[40] https://policy.pinterest.com/en/transparency-report
[41] TikTok, *Intellectual Property Removal Requests Report*, 2021, H1 and H2:
https://www.tiktok.com/transparency/en-us/intellectual-property-removal-requests-2021-2/
[42] https://transparency.twitter.com/en/reports/copyright-notices.html#2021-jul-dec
[43] YouTube, *Copyright Transparency Report*, 2021, H1 and H2:
https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-22_2021-1-1_2021-6-30_en_v1.pdf,
https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-22_2021-7-1_2021-12-31_en_v1.pdf.

- **Dailymotion** has not published a transparency report, meaning that this type of data is not publicly available.

Ownership conflicts relating to reference files are settled between rightholders

If an ownership conflict is detected (where more than one rightholder claims or may claim ownership of the rights with respect to the same content) for a given reference file, service providers inform the rightholders about the existence of such a conflict and invite them to resolve the issue. Pinterest specifies that if an ownership dispute arises between the parties, the service will disable both parties' claims until a court ruling has determined the rightful owner of the content. TikTok advises that it has yet to be confronted with this type of situation.

The service providers indicate that they do not perform any matching during the conflict resolution process to avoid any wrongful action against users.

Rightholders explain that they settle conflicts through the CMS solutions, with one music rightholder even claiming to resolve 4,000 conflicts every month.

However, some rightholders reported a difficulty with *INA signature*. Since the solution does not have a CMS, it is hard for rightholders to resolve any conflicts.

Table 7: Availability of a CMS according to existing fingerprinting tools

Tools	Provision of a CMS
Audible Magic	Yes
Content ID	Yes
Copyright Match Tool	Yes
INA signature	No
MediaMatch	Yes
Content Claiming Portal	Yes
Rights Manager	Yes

Source: Arcom

Content-sharing service providers could:

➢ **Recommendation 5**: mention the applicable copyright rules and provide information on the situations in which exceptions to copyright can be made;

* * *

Fingerprint-based content recognition tools appear to satisfy all the parties involved. The rightholders that took part in Arcom's consultation acknowledge a certain level of efficiency in YouTube's solution. Meta's solution is often considered to be satisfactory, but rightholders believe that there is still room for improvement.

Arcom also notes that other service providers have developed solutions, such as TikTok and Pinterest. However, the Authority has not received any feedback about their effectiveness or use.

Finally, Arcom notes that service providers and rightholders need to regularly discuss the operation and use of these tools to ensure that they are understood and used more effectively.

2. Notices received by service providers: the need for swift action

The IPC states that content-sharing service providers must act expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their service, the notified works[44]. Therefore, service providers give rightholders access to so-called "reporting forms" so that they can report and notify a copyright infringement found on the content-sharing service.

Unlike content recognition tools, which take action by identifying content before it is made available online, rightholders send a notice after the content has already been posted to request that the content be kept offline and removed based on the information sent.

Rightholders may send notices in different situations: the service provider has not implemented any content recognition technology (which is especially the case with LinkedIn), the tool was unable to recognise the uploaded content[45], the rightholder has not provided the relevant and necessary information to prevent the content from being made available (such as the fingerprint), especially in the absence of an agreement on disabling access, or in the event that rightholders do not have access to the content recognition tool due to the eligibility conditions stipulated by the service providers.

The figures provided by content-sharing service providers in their transparency reports indicate that rightholders may make extensive use of their takedown notice forms, with a minimum of 100,000 notices received every year for each service (with the exception of LinkedIn, which reported receiving fewer than 3,000).

Sending and processing notices

Infringement notice forms are presented by the online content-sharing service providers that took part in the consultation as a quick and effective tool for reporting copyright infringements and thereby blocking or removing the reported content.

This observation is shared by rightholders that use a provider or which have a dedicated team for notifying content using the reporting forms.

As for the other rightholders, this finding is more restrained. In particular, one audiovisual rightholder stated that it did not submit manual takedown requests due to the amount of time involved, before adding that "*all content-sharing services should offer technological content recognition solutions*".

---

[44] IPC, Art. L. 137-1, III, 1°, c).
[45] According to the tests carried out in the report published by the CSPLA, Hadopi and the CNC, this happens infrequently or in cases where the content has undergone extreme modifications (the playback speed has been doubled, change in the image colour, camera shake, etc.). CSPLA, Hadopi, CNC, *op. cit.*

Table 8: Percentage of manually blocked content upon receiving a notice from rightholders (exploitable data by service provider worldwide in 2021)

	Number of notices received by service provider	Percentage of content blocked or removed upon receiving a notice
LinkedIn	2,600	99%
Meta	2.1 million	85%
TikTok	128,000	50%
YouTube	10.9 million	91.6%

Source: Transparency reports

Tools that are sometimes hard to access

Since the reporting forms are publicly available, Arcom was able to analyse the ease in accessing the forms.

While most rightholders commend YouTube for its easily accessible forms, access to the forms on other platforms, such as LinkedIn and Twitter, seems to be unintuitive and requires an understanding of the sites' architecture, which was also revealed in some rightholders' replies to the questionnaire: "[the forms] *are not often highlighted*," said one rightholder, while another reported "*major difficulties in finding* [a] *contact address".* The last rightholder also mentioned trouble concerning notices for content uploaded to closed groups, particularly on Facebook. In addition, an account is required to access forms on such platforms as LinkedIn, Pinterest, Twitter and YouTube.

Finally, most services also publish an email address for their "DMCA designated agent[46]", to whom takedown requests can be sent directly without using a reporting form or creating an account.

Table 9: Form and dedicated address

Service provider	Reporting form available	Legal basis for the form	Need for an account	Ease of access / access path	Dedicated email address
Dailymotion	Yes	LCEN	No	Dailymotion.com > Help Centre > Copyright & Community Guidelines > Copyright > Report a copyright infringement > Copyright infringement notification > access to the form	notifications@dailymotion.com
Facebook	Yes	DMCA	No	Facebook.com > Help Center > Policies and	ip@fb.com

---

[46] Digital Millennium Copyright Act, signed into US law in 1998.

Service provider	Reporting form available	Legal basis for the form	Need for an account	Ease of access / access path	Dedicated email address
				Reporting > Intellectual Property > Copyright > access to the form	
Instagram	Yes	DMCA	No	Instagram > Help > Privacy, Security & Reporting > How to Report Things > How do I report copyright infringement on Instagram? > access to the form	ip@instagram.com
LinkedIn	Yes	DMCA	Yes	Linkedin.com > Privacy & Terms > Copyright Policy > Notice of Copyright Infringement Form > access to the form	Not known
Pinterest	Yes	DMCA	Yes	Pinterest.co.uk> > Terms of Service > View Privacy Policy & TOS > Copyright > Submit a copyright complaint > access to the form	copyright@pinterest.com
TikTok	Yes	DMCA	No	Tiktok.com > Copyright > Intellectual Property Policy > Copyright Infringement Report > access to the form	copyright@tiktok.com
Twitter	Yes	DMCA	Yes	Twitter.com > Help Center > Contact Us > Help with intellectual property issues > What issue are you having? > access to the form	copyright@twitter.com
YouTube	Yes	DMCA	Yes	Youtube.com > Copyright > Making claims > access to the form	copyright@youtube.com

Source: Websites of the different service providers

> Content-sharing service providers could:
>
> ➤ **Recommendation 6**: ease access to reporting forms, in particular by ensuring better visibility and free access to them.

Verifying the validity of takedown or blocking requests

To substantiate their blocking or takedown request, rightholders must send the necessary information to the service providers.

Forms cannot be processed until they have been confirmed as "valid" by the service providers' dedicated teams. They must also be sufficiently substantiated[47]. These teams check whether the claimant is legitimately allowed to submit the request and whether the information provided (including the URL link of the notified content) can be used to identify the content in question.

The forms offered by the various service providers are similar, with some even allowing claimants to determine the required blocking measure if the request is admissible, which is the case with Dailymotion, Pinterest and YouTube. For example, Pinterest lets rightholders choose between deleting only the infringing pin or all pins featuring the same image.

Rightholders have not notified Arcom of any particular difficulties in completing the forms or providing information.

<p align="center">* * *</p>

In light of the foregoing, Arcom tends to believe that service providers act expeditiously, upon receiving a notice, to disable access to, or to remove from their platforms, the notified works or other subject matter.

Nevertheless, the Authority notes that service providers and rightholders have provided little information in their replies about the fact that service providers may sometimes be required, upon receiving a notice to remove protected works from their services, to make *"their best efforts to prevent their future uploads"* or make *"their best efforts to prevent further uploads of the notified works and other subject matter for which the rightholders have provided relevant and necessary information, either directly or indirectly through a designated third party"* (refer to Article L. 137-2 of the IPC[48]). In the future, the Authority will carry out a more detailed analysis into the implementation and operation of these measures on all the services normally concerned by such measures.

Furthermore, the copyright policies of content-sharing service providers (in their terms of service or reporting forms) mostly refer to the US Digital Millennium Copyright Act (DMCA). Seven of the eight service providers[49] refer to the DMCA, and only one (Dailymotion) to France's Confidence in the Digital Economy Act (LCEN)[50].

---

[47] As stipulated in c) of III of Article L. 137-2 of the IPC.
[48] These provisions are used as a reference for related rights in Article L. 219-2 of the IPC.
[49] Note that seven content-sharing service providers responded to Arcom's consultation for eight services, with Meta replying for its two services (Facebook and Instagram).
[50] Act no. 2004-575 of 21 June 2004 for confidence in the digital economy.

Only one service (TikTok) mentions Article 17 of the Copyright Directive 2019/790 to inform its users of their right to grant authorisation to the service or otherwise indicate their wish to prevent their content from being made available.

It could be useful for content-sharing service providers targeting a European and French audience to inform users about the applicable copyright rules in these regions/countries, especially the rules relating to Article 17 of the Copyright Directive and Articles L. 137-1 et seq. of the IPC.

Furthermore, in the event of a dispute about the follow-up action taken by the service provider in response to the user's or rightholder's complaint, no service provider informs them that they may refer the matter to Arcom[51].

To ensure that users and rightholders are fully informed, and given that content-sharing service providers are targeting a French audience, it would be desirable to mention this possibility.

Content-sharing service providers could:

➤ **Recommendation 7**: inform French users of the copyright rules in France, in particular those resulting from Article 17 of the Copyright Directive and Articles L137-1 et seq. of the IPC;

➤ **Recommendation 8**: specify, in the general conditions of use or in the online dispute forms, the possibility for users and rightholders to refer to Arcom's dispute settlement process, in the event of a dispute.

---

[51] IPC, Art. L. 137-4.

3. Agreements between rightholders and service providers

There is nothing new about providing remuneration for the dissemination (or preventive blocking) of content protected by copyright and related rights on content-sharing services. Such arrangements had already given rise to the first agreements between the parties involved before the Directive of 17 April 2019 became effective and was incorporated into national law.

For example:
- Dailymotion entered into a single agreement with copyright collection societies SACD (Society of Dramatic Authors and Composers), SCAM (Civil Society of Multimedia Authors), ADAGP (Society of Visual Artists)[52] and SACEM (Society of Authors, Composers and Publishers of Music) in 2008[53]
- Meta had an agreement with SACEM in 2018[54], followed by SCAM[55] and SACD[56] in 2022
- YouTube entered into agreements with SACEM[57], SCAM, SACD and ADAGP in 2010[58]

These licensing agreements (almost all have been renewed) were aimed at allowing the platforms to make the protected content available while promoting and remunerating the authors for the use of their works by users of these services.

The adoption of the Directive of 17 April 2019 and its incorporation into national law have prompted other content-sharing service providers to enter into agreements, or those with existing agreements (such as Meta) to enter into further agreements to avoid any liability for the unauthorised exploitation of protected content on their platforms.

Two types of agreement can be identified:
- Exploitation agreements are aimed at allowing content to be made available and remunerating authors, potentially involving the use of content recognition tools and especially their tracking and monetisation features, as well as providing for rightholders to disable access if they consider, for example, that the exploitation of their content in certain contexts infringes their moral rights.

- Agreements to consistently disable access if rightholders do not want to see their content used on the services. In most cases, this situation requires the use of the content recognition tools implemented by the service providers to detect and disable access to the relevant works.

In accordance with applicable legislation, the absence of an agreement between rightholders and service providers (whether or not aimed at authorising content to be shared by users) does not exempt service providers from making best efforts to ensure the unavailability of specific works for which the rightholders have provided them with the

---

[52] https://www.scam.fr/actualites-ressources/communique-accord-historique-entre-dailymotion-et-les-auteurs/.
[53] https://www.zdnet.fr/actualites/droits-d-auteurs-la-sacem-et-dailymotion-renouvellent-leur-accord-pour-2-ans-39758732.htm.
[54] https://www.francetvinfo.fr/culture/musique/facebook-signe-avec-la-sacem-pour-remunerer-les-artistes_3386311.html.
[55] https://www.scam.fr/uploads/2022/05/CP-accords-Meta-Scam_VFR.pdf.
[56] https://www.sacd.fr/fr/signature-dun-accord-entre-meta-et-la-sacd.
[57] https://www.lemonde.fr/culture/article/2010/09/30/un-accord-entre-la-sacem-et-youtube-garantit-la-remuneration-des-auteurs_1418022_3246.html.
[58] https://www.numerama.com/politique/17453-youtube-signe-un-accord-retroactif-avec-trois-societes-de-gestion.html.

relevant and necessary information. Once again, this often involves the use of automated content recognition solutions.

Furthermore, content subject to exceptions should not, by definition, be blocked even if identified by the recognition tools. Although the number of user disputes remains low, rightholders should produce and provide reference information about the copyright and its exceptions to avoid any conflicts.

Therefore, the technological measures for identifying works and the content recognition tools examined in this report underlie the various issues at stake, whether or not there is an agreement between rightholders and service providers, and regardless of whether users of the services concerned are authorised to share content.

The agreements concluded

Most of the content-sharing service providers have entered into agreements with music and audiovisual rightholders to use their content

Two of the seven service providers who answered the questionnaire did not specify whether they had entered into agreements with rightholders.

However, the five services claiming to have exploitation agreements with rightholders (Dailymotion, Meta, Pinterest, TikTok and YouTube) failed to indicate the number of agreements and whether they cover all cultural sectors, but they did explain that they mainly have agreements with music and audiovisual rightholders.

The exploitation agreements that service providers have concluded with music rightholders involve record companies (or other licensors such as distributors), music publishers and collective management organisations (notably SACEM). One service provider (TikTok) states that its licensing strategy is particularly music-oriented, while another (Meta) advises that it has ties with various distribution companies allowing independent labels and artists to license their content.

The agreements signed with rightholders in the audiovisual sector involve television channels and film studios (respondents did not specify the channels and studios concerned) or, as TikTok states, "*with media and audiovisual partners for specific projects or campaigns*".

Pinterest indicates that it regularly negotiates exploitation agreements with content creators and image catalogue holders. The service also points out that the licensing market for images is not based on the simplified licensing system that exists for other types of content, such as music. According to Pinterest, the market tends to lack structure, and rightholders come from a wide range of backgrounds (individual bloggers, designers taking selfies, cooks sharing photos of their food and professional photographers). However, it should be noted that an agreement between YouTube and ADAGP has existed since 2010 concerning graphic and plastic arts.

None of the service providers gave details about the content of their agreements, although some indicate that monetising content is the main objective.

Finally, when asked about the reasons for not entering into exploitation agreements, service providers explain that there may be commercial disagreements, especially where remuneration demands are excessive in relation to the amount of content available on the services, or that rightholders sometimes fail to respond to their requests.

Only 11 of the 50 rightholders who answered the questionnaire stated that they had entered into exploitation or blocking agreements with service providers. Those 11 rightholders mainly come from the audiovisual sector (50% of the respondents from that sector) and music (45%).

Five audiovisual rightholders claim to have entered into an agreement with YouTube (three to block content, and two to use content), and two rightholders have reached an agreement with Meta for its Facebook and Instagram services (one to block content, and one to use content).

Rightholders in the music sector have entered into the most agreements with service providers: five rightholders advise that they have usage agreements with YouTube, Meta and TikTok, four with SoundCloud, three with Twitch and two with Snapchat.

In all, Arcom was notified of 39 agreements (either for authorising or blocking content)[59]. They have been concluded with eight different service providers (thirty for music rightholders and nine for audiovisual rightholders). YouTube and Meta's services (Facebook and Instagram) are the platforms that have concluded the most agreements with rightholders.

Table 10: Number of agreements with service providers as reported by the rightholders

Service providers reporting that they have entered into agreements	Number of rightholders indicating that they have concluded agreements to authorise or block content	
	Audiovisual (out of 10 respondents)	Music (out of 11 respondents)
Dailymotion	1	1
Meta (Facebook and Instagram)	3 (2 for Facebook, 1 for Instagram)	10 (5 for Facebook, 5 for Instagram)
Pinterest	0	0
TikTok	0	5
YouTube	5	5
Snapchat	0	2
SoundCloud	0	4
Twitch	0	3
TOTAL	9	30

Source: Arcom

The rightholders who answered the questionnaire did not explain their reasons for not entering into agreements. However, it could be assumed that commercial disagreements are to blame, as stated by the service providers, but in some cases it could simply be due to a lack of contact between the parties.

---

[59] Based on the information provided by all respondents, Arcom cannot determine how many of the agreements concluded are for authorising or blocking content.

Some agreements exist between the photography sector and service providers

ADAGP concluded an exploitation agreement with Dailymotion in 2008 and another agreement with YouTube in 2010. Although the agreement with YouTube was renewed in 2018, Arcom has no information about the term of the agreement with Dailymotion.

In 2021, ADAGP and SAIF (Authors' Society for Visual Arts and Still Images) signed a 10-year agreement with Google to support and remunerate authors of graphic, plastic and photographic arts in the digital realm.

Rightholders in the publishing sector have not concluded agreements with content-sharing service providers

The publishing sector appears to be the only respondent that did not report any agreements with service providers, due to the lack of contact from service providers with publishers or their representative bodies. One respondent even considered that "*service providers are responsible for exercising due diligence and reaching out to rightholders*".

## Purpose of the agreements

The main purpose of the agreements concluded by rightholders is to monetise their content

The main reasons why rightholders enter into agreements include monetisation (92% of the agreements concluded), tracking viewership of their online content (81%) and lastly blocking (64%).

Audiovisual rightholders, including television publishers, prioritise agreements for blocking content (67% of the agreements concluded), while music rightholders, who are mainly collective management organisations and record companies, prefer exploitation agreements and therefore monetisation (90%).

These agreements mainly concern YouTube, Facebook, Instagram, TikTok and SoundCloud.

Figure 10: Purpose of the agreements by service provider[60]

B Agreement to block	**M** Agreement to monetise	**T** Agreement to track
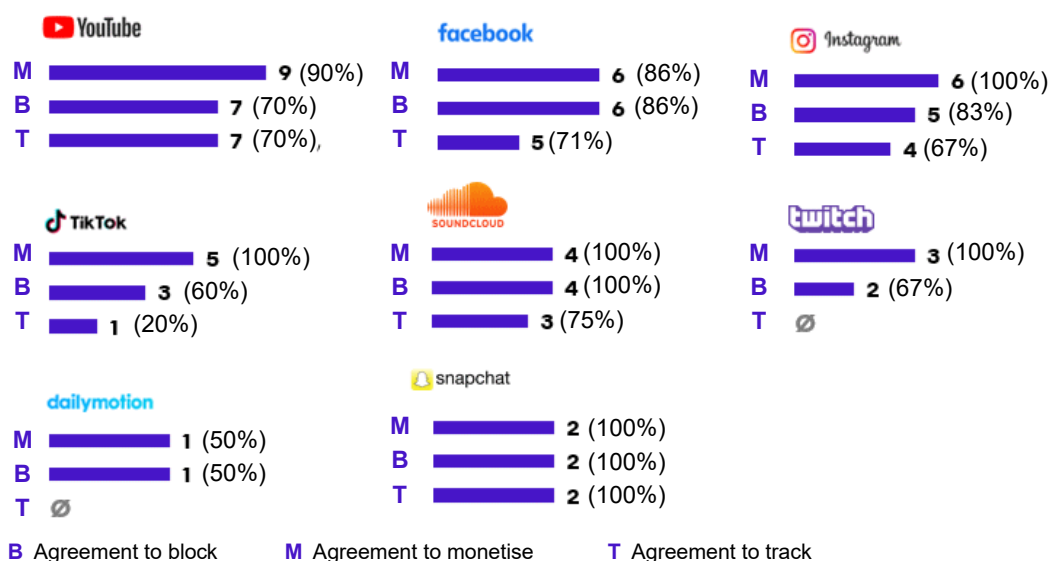
Base: 11 respondents to Q8. Has your company entered into agreements with the following content-sharing services and social media platforms, whether to block, monetise or track your works?

Source: Ifop study for Arcom, 2022

Rightholder satisfaction with the agreements concluded

Rightholders in the audiovisual sector tend to be satisfied with what they claim to be the effective and appropriate agreements concluded with YouTube. However, they did not comment on the agreements with other service providers.

Overall, music rightholders also find the agreements to be effective and satisfactory, and some even report that they are "*essential*". One rightholder states that "*the licensed partners (...) have made efforts to identify the content (...) within the content posted by users*". Therefore, concluding agreements with rightholders seems to give service providers easier control over uploaded content.

Table 11: Rightholders' views about their agreements with content-sharing service providers[61]

	Very	Somewhat	Not really	Not at all
Satisfactory	2	10	2	5
Appropriate	1	11	1	5
Useful	6	6	1	5
Effective	2	11	1	4

Base: 19 respondents to Q.10: Do you believe that the agreements are satisfactory, appropriate, useful and effective?

Source: Ifop study for Arcom, 2022

---

[60] Note on Figure 11: 90% of the agreements reported with YouTube (i.e. nine agreements reported out of all the rightholders who replied to the questionnaire) concern monetisation. As for Facebook, 86% of the agreements reported (i.e. six agreements out of all the rightholders) involve tracking.

[61] Note: 19 respondents answered Q. 10, but they did not complete all the items.

Closer look at... YouTube Creator Music

YouTube launched its *Creator Music* programme at the end of 2022, which allows video creators to apply for monetisation of their videos even if they contain copyright-protected content. According to YouTube, "*Creator Music is a growing catalogue of high-quality music that creators can use in videos without losing monetisation. Some songs can be licensed upfront, allowing creators to retain full monetisation. Other songs may be eligible to share revenue with the track's rightholders*." »

This new feature seems to respect copyright and will probably lead to fewer copyright infringement notices on YouTube, since video creators can obtain a prior licence to use the protected content depending on the track, in return for paying an upfront fee to the track's rightholders, or benefit from a revenue sharing arrangement (revenue from monetising the video will then be split between the track's rightholders and the video creator, after deducting YouTube's share). Until now, rightholders could only submit a request to block the video or receive a share of the revenue generated by YouTubers.

***

Arcom welcomes the existence of agreements between content-sharing service providers and rightholders in the audiovisual, music, photography and graphic arts sectors.

Nevertheless, the Authority notes that these agreements especially concern the main service providers (particularly YouTube and Meta) and the rightholders with the ability to negotiate and contract with them. However, developing greater use of licensing or blocking agreements between all identified service providers and rightholders with smaller catalogues is essential for providing content-sharing platform users with access to a wider range of content, as well as blocking content that rightholders do not want to see made available on these platforms.

Similarly, Arcom notes the lack of agreements between service providers and rightholders in the publishing sector and, more generally, the lack of contact from service providers with those rightholders for the purpose of identifying which practices can be implemented to protect their works, especially audio and digital books.

Furthermore, efforts to conclude agreements with rightholders tend to vary between the different service providers. Some service providers still have a low number of known agreements with rightholders, although there is no way to determine whether they have actually made efforts to conclude new agreements.

Generally, Arcom considers that all service providers still need to make an effort to enter into agreements with the rightholders in the various cultural sectors that took part in the consultation. Special attention should be given to the publishing sector.

Rightholders could:

➢ **Recommendation 9**: produce reference information about the copyright and its exceptions to enable content-sharing service providers to make such information available.

➢ **Recommendation 10**: systematically pursuit the conclusion of agreements, in particular with regard to rightholders in photography and publishing.

Conclusion

This report reveals that the service providers who answered the questionnaire have generally implemented the tools required to ensure compliance with most of the provisions in Article L. 137-2 of the IPC.

Several agreements have been signed and content recognition technologies have been rolled out on the most important content-sharing services, thereby helping identify and monetise content or block infringing content, which is generally an encouraging trend. Therefore, these services can guarantee that unauthorised content will not be made available in the future. More generally, all services act expeditiously upon receiving notices from rightholders.

Nevertheless, these efforts deserve to be continued and extended to encompass all service providers, and not just the main services, particularly by ensuring greater communication with rightholders and especially those in sectors other than the audiovisual and music industries (publishing and still image sectors).

Arcom will remain vigilant regarding the implementation of these efforts and believes it is necessary to receive more detailed information in the future to enable it to better fulfill its mission of evaluating the effectiveness of protective measures.

As for the services that did not participate in the consultation, the Authority believes it should point out that it will conduct a further in-depth analysis to determine whether or not they qualify as content-sharing service providers.

The same applies to the services that informed the Authority that they do not consider themselves to be content-sharing service providers and are therefore not bound by the provisions of Article L. 137-2 of the IPC.

➢ **Recommendation 11**: ensure that Arcom is provided with all the answers it needs to carry out its evaluations;

➢ **Recommendation 12**: inform Arcom of the agreements concluded;

➢ **Recommendation 13**: both parties could continue to collaborate with the goal of concluding agreements and open these agreements to all cultural sectors.