AAPA Recommendations to IMCO Committee Members in relation to the Digital Service Act (DSA) and the Fight against Audiovisual Piracy

June 2021

Introduction

The Audiovisual Anti-Piracy Alliance (AAPA) represents companies involved in the provision of protected audiovisual services, security technology for protecting such services and the manufacturing of products which facilitate the delivery of these services.

Our membership includes the whole audiovisual value chain, such as rightsholders, platform operators, telecommunication companies, OTT providers, broadcasters and technical service providers. Many of our members are global businesses. Our aim is to tackle piracy, particularly pertaining to the development, promotion, distribution, application or use of technologies aimed at allowing illegal access to content.

As described in the Annex, **audiovisual piracy involves severe damaging consequences for the entire audiovisual sector and even beyond.** Indeed, the audiovisual sector remains one of the most impacted sectors for copyright infringements and piracy. The massive illicit consumption of audiovisual services concerns all types of content, ranging from sport competitions to films and TV series. What is more, audiovisual piracy has dramatically accelerated during the pandemic outbreak. The functioning and viability of the whole industry is impacted, leading to a considerable loss of revenue for the entire audiovisual value chain and prejudicing the sustainability of the creative ecosystem and, ultimately, cultural diversity.

Against this background, APA members ask for an urgent and strong response from the IMCO Committee to reinforce the fight against illegal audiovisual content online through the Digital Service Act (DSA).

AAPA Recommendations

More specifically, AAPA members call on IMCO members to:

1. **Clarify the definition of "hosting services" to ensure a more efficient fight against audiovisual piracy**

The definition of "**hosting service**" should be expanded to include services that not only store information but also enable the allowance of storage of information, including services that consist in the provision of IP addresses allowing the anonymous use of domain names and websites. This would include in the scope of the definition, technical services that facilitate piracy by allowing illegal streaming site hosting solutions to be put in place. These include dedicated servers[1], rental service providers, and reverse proxies[2], where currently there is an uncertainty regarding the liability regime

[1] "Dedicated servers" are hosting services in which a physical server is dedicated to a single business customer.

[2] A "reverse proxy" is a common type of proxy server (i.e. a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources) that is accessible from the public

applicable to them. To be fully effective in the fight against illegal content and audiovisual piracy, the DSA should thus explicitly qualify these services as hosting service providers.

This point is expanded upon with concrete wording in our proposed **Amendment 1.**

2. Avoid jeopardising expeditious withdrawals of notified illegal content

We very much support the idea that providers of hosting services shall, upon obtaining actual knowledge or awareness, remove or disable access to illegal content as soon as possible.

Against this background, we strongly oppose the proposal made by your rapporteur in her amendment 71, which requests hosting services to remove or disable access to illegal content which does not seriously harm public policy, public security, public health or consumers' health or safety within seven days. While we do recognise the intention to clarify that different types of content may require different removal deadlines, in our view, seven days cannot be considered as an expeditious withdrawal. This would be extremely detrimental to the whole audiovisual sector which is already struggling to ensure that flagged illegal content is taken down rapidly, and would only increase audiovisual piracy in the EU.

A very good example of why a 7-days deadline is not acceptable, is live sports or entertainment events, whose economic value lies almost entirely in the live component. The removal or disabling of access to illegal broadcasts of live content should be done as quickly as possible and definitively before the end of the match or concert or live show, an assessment shared by the European Parliament's resolution that was adopted on 19 May 2021.

We also refute your rapporteur's justification, according to which digital platforms would need time to assess the legality of content before taking it down. Indeed, audiovisual broadcasts are usually finger-printed and/or watermarked, so that illegal transmissions are easily and swiftly identified without any room for interpretation on their illegality.

Therefore, AAPA urge IMCO members to delete amendment 71 proposed by your rapporteur.

3. Adopt measures to fight the facilitation of "off-platforms infringement"

One of the big issues with the major online content sharing platforms (e.g. YouTube or Facebook) currently is not just the illegal content stored on their platform, but rather the material posted on their platform that directs users to other places which supply illegal content (e.g. by listening to tutorial video or by following hyperlinks in the videos, or in the comments, to streaming websites).

As long as the illicit content is not stored on the online platform, the EU's Copyright Directive (2019/790) cannot apply. Today, indirect access to illicit contents via hyperlinks shared on online content-sharing platforms prevails over the consumption of video stored on such platforms.

network. Large websites and content delivery networks use reverse proxies, to balance the load between internal servers. Reverse proxies are typically owned or managed by the web service, and they are accessed by clients from the public internet.

Online content sharing platforms do not tend to see indirect access to illicit content as their problem, while this is highly damaging for rightsholders. Measures should be inserted in the DSA to increase the liability of online content-sharing platforms in this respect, regardless of whether such platforms are considered as active or passive hosting service providers.

This point is expanded upon with concrete wording in our proposed **Amendment 2.**

4. **Adopt harmonised "notice and action" procedures, including stay down measures, specific policies related to trusted flaggers, and actions against repeat infringement**

The Notice & Action procedures would only apply to intermediaries which meet the required conditions to benefit from the limited liability regime foreseen by the e-Commerce Directive. In our view, these procedures should include:

- An obligation of suspension in the event of the reappearance of a content previously taken down - i.e. **"stay down" measures**. For concrete wording, please refer to our proposed **Amendments 3-4.**
- Specific policies listing **trusted flaggers**, defining their role, and enabling fast intervention. For concrete wording, please refer to our proposed **Amendments 5-7.**
- A clear written anti-piracy policy with deterrent **measures against repeat infringement**. For concrete wording, please refer to our proposed **Amendments 8-10.**

5. **Provide for a comprehensive "Know Your Business Customer" obligation**

The AAPA welcomes the IMCO report's extension of the "**Know Your Business Customer**" **obligation to all intermediaries**. We agree that this obligation should apply to all digital services, irrespective of their active or passive nature, making it mandatory to collect the data and verify the identity of business customers wishing to use their services. We therefore encourage the IMCO committee to **preserve this vital obligation** in its final report and throughout the negotiations with the Council of the EU.

Proposed AAPA Amendments on the DSA

Definitions

AAPA amendment 1

Proposal for a regulation

Article 2 (f)

Text proposed by the Commission	*Amendment*
- a 'hosting' service that consists of the storage of information provided by, and at the request of, a recipient of the service;	- a 'hosting' service that consists of the storage ***or the allowance of storage of*** information provided by, and at the request of, a recipient of the service; ***A hosting service also includes a service that consists in the provision of IP address allowing the anonymous use of domain names and websites.***

Justification

Some players play a strategic role in the piracy ecosystem and could, through their actions, help to limit the phenomenon: dedicated server / rental service providers facilitate piracy by allowing illegal streaming site hosting solutions to be put in place; "reverse proxy" service providers are an essential link in the spiderweb woven by pirate sites to organize their anonymity. The "reverse proxy" acts as an IP address scrambler to the rest of the Internet: it provides malicious sites with an IP address that does not match that of the server on which they are hosted. Even though these intermediaries are often the only ones that rights holders are able to identify, there is uncertainty as to the liability regime applicable to them with regard to the mechanisms provided for by the DSA. To be fully effective, the DSA should make it possible to expressly qualify the technical intermediaries mentioned above as hosting service providers within the meaning of Article 2 (f) of the DSA.

Off-platform infringement

AAPA amendment 2

Proposal for a regulation

Article 14 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) **a clear indication of the electronic location of that information, in particular the exact URL or URLs, and** where necessary**,** additional information enabling the identification of the illegal content;	(b) where necessary, additional information enabling the identification of the illegal content ***not only stored on an online platform but also material posted on an online platform that directs users to locations that supply illegal content***;

Justification

One of the major issues with the online content sharing platforms is not just the illegal content stored on their platform, but rather the material posted on their platform that directs users to other places which supply illegal content (e.g. by listening to tutorial video and/or by following hyperlinks in the videos, or in the comments, to streaming websites). Today, indirect access to illicit contents via hyperlinks shared on online content-sharing platforms prevails over the consumption of video stored on such platforms.

Stay-down measures

AAPA amendment 3

Proposal for a regulation

Recital 39a (new)

Text proposed by the Commission	*Amendment*
	(39a) In order to effectively and meaningfully address the proliferation of illegal goods and services online, intermediary services should implement measures to prevent illicit content from reappearing after having been taken down. Such measures, undertaken horizontally by all intermediary services, will contribute to a safer online environment.

Justification

In line with the introduction of the new Article 13a on Measures against the reappearance of illegal content.

AAPA amendment 4

Proposal for a regulation

Article 13a (new) – Measures against the reappearance of illegal content

Text proposed by the Commission	*Amendment*
	Article 13a
	Measures against the reappearance of illegal content
	Where an intermediary service detects and identifies illegal goods or services, it shall prevent this content from reappearing on its service. The application of this requirement shall not lead to any general monitoring obligation.

Justification

In order to effectively and meaningfully address the proliferation of illegal products and services on intermediary services, measures need to be implemented by these services to prevent illicit content from reappearing after having been taken down. Such measures, undertaken horizontally by all intermediary services, will contribute to a safer online environment.

Trusted flaggers

AAPA amendment 5

Proposal for a regulation

Recital 46

Text proposed by the Commission	*Amendment*
(46) Action against illegal content can be taken more quickly and reliably where ***online platforms*** take the necessary measures to ensure that notices submitted by trusted flaggers through the notice and action mechanisms required by this Regulation are treated with priority, without prejudice to the requirement to process and decide upon all notices submitted under those mechanisms in	(46) Action against illegal content can be taken more quickly and reliably where ***hosting services*** take the necessary measures to ensure that notices submitted by trusted flaggers through the notice and action mechanisms required by this Regulation are treated with priority, without prejudice to the requirement to process and decide upon all notices submitted under those mechanisms in a timely, diligent, objective and effective manner. Such

a timely, diligent and objective manner. Such trusted flagger status should only be awarded to entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content, that they represent collective interests and that they work in a diligent and objective manner. Such entities can be public in nature, such as, for terrorist content, internet referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation ('Europol') or they can be non-governmental organisations and semi- public bodies, such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online. For intellectual property rights, organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions. The rules of this Regulation on trusted flaggers should not be understood to prevent online platforms from giving similar treatment to notices submitted by entities or individuals that have not been awarded trusted flagger status under this Regulation, from otherwise cooperating with other entities, in accordance with the applicable law, including this Regulation and Regulation (EU) 2016/794 of the European Parliament and of the Council.

trusted flagger status should be awarded to entities, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content, ***have significant legitimate interests, have a proven record in flagging content with a high rate of accuracy and particular expertise and have demonstrated competence for the purposes of detecting, identifying and notifying illegal content.*** Such entities can also be public in nature, such as, for terrorist content, internet referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation ('Europol') or they can be non-governmental organisations and semi-public bodies, such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online. For intellectual property rights, organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions. The rules of this Regulation on trusted flaggers should not be understood to prevent online platforms from giving similar treatment to notices submitted by entities or individuals that have not been awarded trusted flagger status under this Regulation, from otherwise cooperating with other entities, in accordance with the applicable law, including this Regulation and Regulation (EU) 2016/794 of the European Parliament and of the Council.

Justification

Amended in line with the changes made under Article 15a.

AAPA amendment 6

Proposal for a regulation

Article 15a (new) – Trusted Flaggers

Text proposed by the Commission	*Amendment*
	Article 15a
	Trusted flaggers
	1. Hosting services shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers through the mechanisms referred to in Article 14, are processed and decided upon with priority and without delay, and within maximum 30 minutes where the illegal content pertains to the broadcast of a live sports or entertainment event.
	2. The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the hosting provider or the Digital Services Coordinator of the Member State in which the applicant is established, where the applicant has demonstrated to meet all of the following conditions:
	(a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;
	(b) or it has a significant legitimate interest, either collectively or as individual entity, is independent from any online platform, and has a proven expertise of flagging illegal content with a high rate of accuracy;
	(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.
	3. Digital Services Coordinators shall communicate to the Commission and the Board the names, addresses and electronic mail addresses of the entities to which they have awarded the status of the trusted flagger in accordance with paragraph 2.
	4. The Commission shall publish the information referred to in paragraph 3 in a publicly available database and keep the database updated.
	5. Where a hosting service has information indicating that a trusted flagger submitted a

significant number of wrongful notices through the mechanisms referred to in Article 14, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 17(3), it shall communicate that information to the Digital Services Coordinator that awarded the status of trusted flagger to the entity concerned, providing the necessary explanations and supporting documents.

6. The Digital Services Coordinator that awarded the status of trusted flagger to an entity shall revoke that status if it determines, following an investigation either on its own initiative or on the basis information received by third parties, including the information provided by a hosting service pursuant to paragraph 5, that the entity no longer meets the conditions set out in paragraph 2. Before revoking that status, the Digital Services Coordinator shall afford the entity an opportunity to react to the findings of its investigation and its intention to revoke the entity's status as trusted flagger.

7. The Commission, after consulting the Board, may issue guidance to assist hosting services and Digital Services Coordinators in the application of paragraphs 5 and 6.

Justification

To ensure consistency with the harmonisation objective of the Regulation, Article 19 from Section 3 of Chapter III should be moved to Section 2 of Chapter III, in a new Article 15a. The Trusted flagger system should therefore become a standard for all hosting service providers. This extension will contribute to the overall aim of the DSA to reduce illegal content whilst serving as an effective instrument in the fight against online piracy. The removal or disabling of access to illegal broadcasts of live content should be done "with priority and without delay" and in any event no later than within 30 minutes of the receipt of the notification from a trusted flagger regarding the existence of such illegal broadcast, as recommended by the European Parliament resolution on "on challenges of sport events' organisers in the digital environment" that was adopted on 19 May 2021. We welcome the Commission's proposal to formalise the attribution of such a status by involving an independent third party (the Digital Services Coordinators), but based on established practices, hosting services should also continue to be able to appoint trusted flaggers. Indeed, some have similar systems in place and collaboration can work. Shifting attribution entirely to DSCs would slow the process down and represent a step back. The requirement that a trusted flagger should represent collective interests in Art. 19.2(b) has to be deleted, as such a provision would not qualify individual right-holders (and third parties operating notices on their behalf) as trusted flaggers, although they have been at the forefront of the development and evolution of notice and

action mechanisms. This is a retrograde step from the position today and should be corrected. It is imperative that broadcasters be clearly included, so as to preserve their IPR commitments and uphold their rights.

AAPA amendment 7

Proposal for a regulation

Article 19

Text proposed by the Commission	*Amendment*
Article 19	
Trusted Flaggers	
1. Online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers through the mechanisms referred to in Article 14, are processed and decided upon with priority and without delay. ***2. The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the Digital Services Coordinator of the Member State in which the applicant is established, where the applicant has demonstrated to meet all of the following conditions:*** ***(a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;*** ***(b) it represents collective interests and is independent from any online platform;*** ***(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.*** ***3. Digital Services Coordinators shall communicate to the Commission and the Board the names, addresses and electronic mail addresses of the entities to which they have awarded the status of the trusted flagger in accordance with paragraph 2.*** ***4. The Commission shall publish the information referred to in paragraph 3 in a***	***deleted***

publicly available database and keep the database updated.
5. Where an online platform has information indicating that a trusted flagger submitted a significant number of insufficiently precise or inadequately substantiated notices through the mechanisms referred to in Article 14, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 17(3), it shall communicate that information to the Digital Services Coordinator that awarded the status of trusted flagger to the entity concerned, providing the necessary explanations and supporting documents.
6. The Digital Services Coordinator that awarded the status of trusted flagger to an entity shall revoke that status if it determines, following an investigation either on its own initiative or on the basis information received by third parties, including the information provided by an online platform pursuant to paragraph 5, that the entity no longer meets the conditions set out in paragraph 2. Before revoking that status, the Digital Services Coordinator shall afford the entity an opportunity to react to the findings of its investigation and its intention to revoke the entity's status as trusted flagger
7. The Commission, after consulting the Board, may issue guidance to assist online platforms and Digital Services Coordinators in the application of paragraphs 5 and 6.

Justification

Deleted in line with the changes made under Article 15a.

Repeat infringer policy

AAPA amendment 8

Proposal for a regulation

Article 15 b (new)

Text proposed by the Commission	*Amendment*
	Article 15b
	Measures and protection against misuse
	1. Hosting services shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide or facilitate the dissemination of illegal content. In cases of repeat suspension, providers of hosting services shall terminate the provision of their services and introduce mechanisms that prevent the re-registration of recipients of service that frequently provide or facilitate the dissemination of illegal content.
	2. Hosting services shall terminate after having issued a prior warning, the processing of notices and complaints submitted through the notice and action mechanisms and internal complaints-handling systems referred to in Articles 14 and 17, respectively, by individuals or entities or by complainants that frequently submit notices or complaints that are manifestly unfounded.
	3. Hosting services shall assess, on a case-by-case basis and in a timely, diligent and objective manner, whether a recipient, individual, entity or complainant engages in the misuse referred to in paragraphs 1 and 2, taking into account all relevant facts and circumstances apparent from the information available to the intermediary service. Those circumstances shall include at least the following:
	(a) the absolute numbers of items of illegal content or unfounded notices or complaints, submitted in the past year;
	(b) the relative proportion thereof in relation to the total number of items of information provided or notices submitted in the past year;

	(c) the gravity of the misuses and its consequences; ***(d) the intention of the recipient, individual, entity or complainant.*** ***4. Hosting services shall set out, in a clear and detailed manner, their policy in respect of the misuse referred to in paragraphs 1 and 2 in their terms and conditions, including as regards the facts and circumstances that they take into account when assessing whether certain behaviour constitutes misuse and the duration of the suspension.***

Justification

To ensure consistency with the harmonisation objective of the Regulation, Article 20 from Section 3 of Chapter III should be moved to Section 2 of Chapter III, in a new Article 15b. This extension will contribute to the overall aim of the DSA to reduce illegal content whilst serving as an effective instrument in the fight against online piracy. As part of this, when a hosting service decides to suspend a user, that service should do its utmost to prevent the user from reappearing on the service until the user's suspension has been lifted. Additionally, when a user frequently provides notices or complaints that are manifestly unfounded, the processing of notices and complaints submitted by that user should be terminated by the hosting service.

AAPA amendment 9

Proposal for a regulation

Article 20

Text proposed by the Commission	*Amendment*
Article 20	
Measures and protection against misuse	
1. Online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content. ***2. Online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the processing of notices and complaints submitted through the notice and action mechanisms and internal complaints-handling systems referred to in Articles 14 and 17, respectively, by individuals or entities or by complainants that***	***deleted***

frequently submit notices or complaints that are manifestly unfounded.
3. Online platforms shall assess, on a case-by-case basis and in a timely, diligent and objective manner, whether a recipient, individual, entity or complainant engages in the misuse referred to in paragraphs 1 and 2, taking into account all relevant facts and circumstances apparent from the information available to the online platform. Those circumstances shall include at least the following:
(a) the absolute numbers of items of manifestly illegal content or manifestly unfounded notices or complaints, submitted in the past year;
(b) the relative proportion thereof in relation to the total number of items of information provided or notices submitted in the past year;
(c) the gravity of the misuses and its consequences;
(d) the intention of the recipient, individual, entity or complainant.
4. Online platforms shall set out, in a clear and detailed manner, their policy in respect of the misuse referred to in paragraphs 1 and 2 in their terms and conditions, including as regards the facts and circumstances that they take into account when assessing whether certain behaviour constitutes misuse and the duration of the suspension.

Justification

Deleted in line with the changes made under Article 15b.

AAPA amendment 10

Proposal for a regulation

Recital 47

Text proposed by the Commission	*Amendment*
(47) The misuse of services of ***online platforms*** by frequently providing ***manifestly*** illegal	(47) The misuse of services of ***hosting services*** by frequently providing illegal content or by

content or by frequently submitting manifestly unfounded notices or complaints under the mechanisms and systems, respectively, established under this Regulation undermines trust and harms the rights and legitimate interests of the parties concerned. Therefore, there is a need to put in place appropriate and proportionate safeguards against such misuse. Information should be considered to be ***manifestly*** illegal content and notices or complaints should be considered manifestly unfounded where it is evident to a layperson, without any substantive analysis, that the content is illegal respectively that the notices or complaints are unfounded. Under certain conditions, ***online platforms*** should temporarily suspend their relevant activities in respect of the person engaged in abusive behaviour. This is without prejudice to the freedom by ***online platforms*** to determine their terms and conditions and establish stricter measures in the case of manifestly illegal content related to serious crimes. For reasons of transparency, this possibility should be set out, clearly and in sufficiently detail, in the terms and conditions of the ***online platforms***. Redress should always be open to the decisions taken in this regard by online platforms and they should be subject to oversight by the competent Digital Services Coordinator. The rules of this Regulation on misuse should not prevent ***online platforms*** from taking other measures to address the provision of illegal content by recipients of their service or other misuse of their services, in accordance with the applicable Union and national law. Those rules are without prejudice to any possibility to hold the persons engaged in misuse liable, including for damages, provided for in Union or national law.

	frequently submitting manifestly unfounded notices or complaints under the mechanisms and systems, respectively, established under this Regulation undermines trust and harms the rights and legitimate interests of the parties concerned. Therefore, there is a need to put in place appropriate and proportionate safeguards against such misuse. Information should be considered to be illegal content and notices or complaints should be considered manifestly unfounded where it is evident to a layperson, without any substantive analysis, that the content is illegal respectively that the notices or complaints are unfounded. Under certain conditions, ***hosting services*** should temporarily suspend their relevant activities in respect of the person engaged in abusive behaviour. This is without prejudice to the freedom by ***hosting services*** to determine their terms and conditions and establish stricter measures in the case of manifestly illegal content related to serious crimes. For reasons of transparency, this possibility should be set out, clearly and in sufficiently detail, in the terms and conditions of the ***hosting services***. Redress should always be open to the decisions taken in this regard by online platforms and they should be subject to oversight by the competent Digital Services Coordinator. The rules of this Regulation on misuse should not prevent ***hosting services*** from taking other measures to address the provision of illegal content by recipients of their service or other misuse of their services, in accordance with the applicable Union and national law. Those rules are without prejudice to any possibility to hold the persons engaged in misuse liable, including for damages, provided for in Union or national law.

Justification

The recital is adapted in line with the changes made under Article 15b.

Annex

Challenges related to the fight against audiovisual piracy in the EU

1. Piracy involves severe damaging consequences for the entire audiovisual sector and even beyond

According to a recent EUIPO report on Online Copyright Infringement in the EU[3],. The report pointed out that the average internet user in the EU accessed pirated content 9.7 times per month in 2018 and that TV copyright infringement represented nearly 60% of the total, followed by film and music piracy.

The audiovisual sector remains one of the most impacted sectors for copyright infringements and piracy. There are in fact two types of piracy impacting the whole audiovisual sector:

- piracy of audiovisual services: unlawful access to entire channels offerings or to specific channels (e.g. via Internet Protocol Television (IPTV) – see below) directly impacting audience or the number of subscribers for broadcasters;
- piracy of audiovisual content: illicit access to content like sports competitions, films and series (e.g. via live streaming, streaming, direct download, peer-to-peer) which impacts the attractiveness of the legal offer in which legitimate providers significantly invest.

The massive illicit consumption of audiovisual services concerns all types of content, ranging from sport competitions to films and TV series. Piracy generally occurs on premium content for which the consequences are even more damaging because it undermines the high value and the exclusivity of their distribution. The functioning of the whole industry is impacted, leading to a **considerable loss of revenue for the entire audiovisual value chain**, including AAPA members, and prejudicing the sustainability of the creative ecosystem and, ultimately, cultural diversity.

There are also various ways in which IP infringements financially support the emergence of other types of crime. The latest joint report by EUROPOL and EUIPO presents examples revealing the direct connection between IP crime and a wide range of other forms of organised criminality, including money laundering, document fraud, cybercrime, fraud, drug production, trafficking and terrorism[4].

2. The example of an increasingly sophisticated criminal technology: Internet Protocol Television (IPTV) piracy

Among all these practices, one distinguishes itself from the others due to its steady proliferation: IPTV piracy.

---

[3] *Online Copyright Infringement in the European Union - Music, Films and TV (2017-2018), Trends and Drivers*, EUIPO - European Union Intellectual Property Office, November 2019, https://euipo.europa.eu/ohimportal/en/web/observatory/online-copyright-infringement-in-eu.

[4] *IP crime and its link to other serious crimes - Focus on Poly-Criminality*, EUROPOL and EUIPO joint case book, June 2020, https://www.europol.europa.eu/publications-documents/ip-crime-and-its-link-to-other-serious-crimes-focus-poly-criminality

IPTV is a technology that allows live and on-demand streaming of television content online. It has led to a shift amongst broadcasters from traditional modes of broadcasting by air, satellite and cable towards internet-based streaming. While it offers advantages to customers as broadcasters & TV platforms are able to offer flexible online access and video on demand, criminals have taken advantage of the expanding market and the increasing number of subscribers to set up illegal IPTV platforms. Both the barriers for criminals to enter this market and the corresponding penalties are low, while the rewards are high. In other words, IPTV piracy is a low risk, high return business.

IPTV piracy represents now the most rapidly expanding means of illegal access. Criminals make it possible to watch audiovisual content online through a TV-connected Android box which allows users to access thousands of pay channels by purchasing an illegal subscription at a very low price. In the past, pirated contents were available only in poor quality on insecure websites and/or required downloading risky files from peer-to-peer. IPTV has brought piracy into the home and directly on to the TV as users require minimal technical knowledge to set it up. Using familiar social messaging platforms like WhatsApp, Viber or Discord to operate customer services, communication apps are ensuring frictionless access to pirate services.

3. A phenomenon which dramatically accelerated during the pandemic outbreak

While millions of people were (and still are, to some extent) locked down at home, looking for different types of digital entertainment to cope with social isolation, criminals have exploited the crisis and adapted their operations to expand their illegal activities.

EUROPOL recently shared concerns about the capacity of criminals to adapt their pirate IPTV offers to global lockdown measures during the Covid-19 outbreak. Pirate offers have increased in number and quality, taking advantage of the lack of sport events and the reduction in the stream quality being delivered by legitimate providers due to EU broadband overload[5].

Furthermore, a loss of quality and a declining response rate from online intermediaries to notices during the crisis has been observed. Fighting against piracy should not be affected by any external factors like remote working conditions. Adequate means should be provided to make sure online platforms[6] adapt to all situations, especially in times of crisis, in order to maintain a sufficient level of involvement and responsiveness. The challenge is to develop and ensure the implementation of tools that are sufficiently secure for use in both remote working situations and at the workplace.

[5] *Covid-19: Illegal Streaming*, dedicated page on EUROPOL website, https://www.europol.europa.eu/covid-19/covid-19-illegal-streaming

[6] The term “online platform” encompasses several categories: UGC platforms, social networks, search engines, online marketplaces, and hosting providers.