EUROPEAN
COMMISSION

Brussels, 22.5.2025
SWD(2025) 132 final

COMMISSION STAFF WORKING DOCUMENT

Counterfeit and Piracy Watch List

TABLE OF CONTENT

1. INTRODUCTION

Infringements of intellectual property rights (IPR), in particular commercial-scale counterfeiting and piracy, are a cause of serious concern for the European Union (EU). IPR infringements not only cause significant financial losses for European rightholders and undermine sustainable business models built on intellectual property, but they also pose a major threat to public health and the society as a whole. For instance, counterfeit medicines, medical supply and equipment can endanger lives, compromise healthcare systems and erode consumer trust in essential goods. In addition, the widespread nature of these infringements weakens innovation and hinders growth of industries that rely on IPR protection.

In line with the stated objectives to fight counterfeiting and piracy[1], the Commission is releasing this fourth edition of the Counterfeit and Piracy Watch List ('the Watch List'), regularly published since 2018. The Watch List is based on the input from stakeholders gathered through a public consultation[2] and contains examples of reported marketplaces or service providers whose operators or owners are allegedly resident outside the EU and which reportedly engage in, facilitate or benefit from counterfeiting and piracy.

The Watch List also includes a separate section on online marketplaces and social media platforms which play an important role in the online environment and are expected to take further measures to combat piracy or counterfeiting, such as applying industry standards and best practices, as well as other measures to prevent IP infringements.

As highlighted by the latest EU customs data[3], the volume of fake products entering the EU remains very high. In 2023, the EU customs authorities seized at EU external borders 17.5 million individual items that infringed IPR. Packaging material, followed by toys, was the leading category in terms of the number of items detained, while watches, followed by bags, wallets, purses and clothing, were the leading category in terms of estimated value. China remains the main source for most fake and counterfeit goods entering the EU in 2023 (main source for clothing and toys), followed by Hong Kong (China) (main source for labels, tags, stickers as well as mobile phones and accessories) and Türkiye (main source for clothing, perfumes and cosmetics). Postal, express and air transport remain the most significant means of transport in terms of the number of consignments registered.

Regarding piracy[4], mixed trends across the different types of content were observed in the EU, but overall piracy stabilized at 10.2 accesses per internet user per month. Streaming remained the dominant method for accessing pirated content. TV piracy remained high and music piracy rose slightly above the 2022 levels. Software piracy also saw a 6% increase, primarily driven by mobile devices. Web-based sports piracy declined slightly, but at the same time internet protocol television (IPTV) piracy, which is a major channel for live sports piracy, rose by 10%, with an estimated 1% of EU internet users subscribing to illegal IPTV services. Publications' piracy

[1] Commission Communication *"A balanced IP enforcement system responding to today's societal challenges"* (COM(2017) 707 final), Commission Communication *"Trade for all"* (COM(2015) 497 final), the *IP Action Plan* (COM(2020) 760 final) and the *Strategy for the Enforcement of Intellectual Property Rights in Third Countries*, (COM(2014) 389 final).

[2] https://policy.trade.ec.europa.eu/consultations/public-consultation-counterfeit-and-piracy-watch-list-1_en. For further details on the public consultation, see Annex II.

[3] European Commission: Directorate-General for Taxation and European Union Intellectual Property Office, *EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2023*, Alicante, 2024, https://taxation-customs.ec.europa.eu/document/download/67bd3b33-c597-47d5-aae9-c7336f60d6fe_en.

[4] EUIPO, *Online copyright infringement in the European Union – films, music, publications, software and TV (2017-2023)*, Alicante, 2023, https://data.europa.eu/doi/10.2814/966644.

remained flat, with manga being the most pirated type of publications. In contrast, film piracy decreased by 25%.

Several studies show the economic harm of piracy on the creative industries. According to some resources looking into the trends in online piracy[5], visits to piracy websites in 2023 increased by 6.7% compared to 2022, with the biggest increase in the software sector, followed by music. According to a 2023 report by the recording industry[6], 29% of listeners used unlicensed or illegal ways to listen to the music.

Besides the economic harm to rightholders, there is a rising threat of dangerous counterfeits creating risks to public health, consumers, and society[7], with the growing role of the digital space in the distribution of counterfeit products (both tangible and non-tangible) to consumers through online platforms, including social media platforms and instant messaging services.

Regarding the different types of dangerous counterfeits, a study by the OECD and the EUIPO[8] shows that the most trafficked counterfeit products include perfumery and cosmetics, clothing, toys, automotive spare parts and pharmaceuticals. A significant portion of these counterfeit goods originate from China (55% of global customs seizures) and Hong Kong (China) (19%). Among dangerous fakes ordered online, cosmetics items were the most common, followed by clothing, toys and automotive spare parts. A large majority (75%) of these goods were shipped from China.

IP crime can also act as a gateway to other serious and organised crimes[9]. Counterfeiting has been identified as a high impact crime in the 2021-2025 EMPACT Priorities[10]. In 2023, over 1400 investigations into IP crime were opened through the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

The aim of this Watch List is to encourage the operators and owners of marketplaces, as well as the responsible local enforcement authorities and governments to take the necessary actions and measures to reduce the availability of IPR infringing goods or services on these marketplaces. In this context, the Commission services will continue using the Watch List in their cooperation with EU's trading partners in the framework of IP Dialogues and Working Groups and in the framework of the EU IP related cooperation activities and programmes. The Watch List also intends to raise consumer awareness concerning the environmental, product safety and other risks of purchasing from potentially problematic marketplaces.

The methodology employed in the preparation of the Watch List is outlined in Annex I, while the details of the results of the public consultation are provided in Annex II to this document.

As in case of the 2022 edition, this edition of the Watch List does not contain updates on online service providers or marketplaces reported for Ukraine, without prejudice to possible concerns with these services or marketplaces.

[5] https://www.muso.com/piracy-by-industry-report-2023
[6] https://www.ifpi.org/wp-content/uploads/2023/12/IFPI-Engaging-With-Music-2023_full-report.pdf
[7] EUIPO/Europol, *IP Crime Threat Assessment 2022*, Alicante, 2022, https://data.europa.eu/doi/10.2814/830719.
[8] OECD/EUIPO, *Dangerous Fakes: Trade in counterfeit goods that pose health, safety and environmental risks*, OECD Publishing, Paris, 2022, https://doi.org/10.1787/117e352b-en.
[9] Europol/EUIPO, *Uncovering the Ecosystem of Intellectual Property Crime: A focus on enablers and impact*, Alicante, 2024, https://data.europa.eu/doi/10.2814/1947113.
[10] https://www.europol.europa.eu/crime-areas-and-statistics/empact

The Watch List is a Commission Staff Working Document. Commission Staff Working Documents are factual and informative documents that **do not have any legal effect** and that **do not commit the European Commission.**

The Watch List is a selection of marketplaces and service providers reported by stakeholders. The name of each marketplace and service provider mentioned is accompanied by a short summary of the allegations of the reporting stakeholders and, where provided, a summary of the response of the mentioned marketplace or service provider to those allegations. The European Commission does not take any position on the content of such allegations and the responses to these allegations.

The Watch List is not an exhaustive list of the reported marketplaces and service providers and does not contain findings of legal violations nor assessments of the compliance with applicable EU rules. The Watch List is limited to reporting on the allegations made by stakeholders and the replies provided by the marketplaces and service providers concerned. The Commission services made every effort to ensure that the information contained in the Watch List reflects accurately and comprehensively the views gathered from all the stakeholders that have participated in the consultation process. The Commission services made every effort to ensure that the information contained in the Watch List is accurate to the best of their knowledge and duly verified, notably through close cooperation between all the relevant Commission services, and the involvement of the European Union Agency for Law Enforcement Cooperation (EUROPOL).

The Commission services made every effort to gather the views of the operators of the relevant marketplaces and service providers included in this Watch List. The Commission services provided them with the opportunity to be heard. In particular, the Commission services invited all relevant stakeholders to submit written contributions to the public consultation launched in June 2024 and following the publication of the submissions, also invited interested stakeholders to make comments on the submissions received.

Moreover, the Commission services proactively reached out to a number of online service providers and marketplace operators to verify information received through the public consultation, where needed. The Commission services took duly into account the comments received from the marketplaces and service providers on the allegations made against them by other stakeholders when drawing up this Watch List. The comments of the service providers and marketplace operators mentioned in this Watch List are summarised together with the allegations of reporting stakeholders.

The Commission services remain available to receive further comments on the information reported in this Watch List as well as requests to rectify this information (e-mail to TRADE-COUNTERFEIT-AND-PIRACY-WATCH-LIST@ec.europa.eu) and will take them into account when regularly updating it in the future.

The Watch List does not provide the Commission services' analysis of the state of protection and enforcement of IPR in the countries connected with the mentioned marketplaces and service providers. A general analysis of the protection and enforcement of IPR in third countries can be found in the Commission services' separate biennial *Report on the protection and enforcement of intellectual property rights in third countries (Third country report*), the latest of which has been published in parallel to this edition of the Watch List.

POSITIVE DEVELOPMENTS SINCE THE 2022 WATCH LIST

Since the 2022 Watch List, several enforcement actions and measures have been taken by enforcement authorities, rightholders and the owners, operators and landlords of marketplaces and online service providers. Some of the marketplaces or service providers mentioned in the 2022 Watch List are therefore no longer mentioned in this Watch List. Others are not mentioned, despite continued concern expressed by rightholders, due to their diminished popularity or relevance. The Commission welcomes these actions and measures and encourages enforcement authorities, rightholders and the owners, operators and landlords to continue combating piracy and counterfeiting. Some concrete examples of these developments are given below.

Positive developments by e-commerce platforms and online services

The 2022 edition of the Watch List reported on progress regarding e-commerce platforms *Mercado Libre*, *Sneapdeal* and *Bukalapak.* These platforms are no longer described in detail in this edition of the Watch List but they will remain under review for further developments. More information on e-commerce platforms is provided in Section 4.

With regard to online services that offer or facilitate access to copyright protected content, several services reported in the 2022 Watch List lost their importance or became unavailable, for example:

- *Flvto.biz* and *2conv.com* - the music industry reports that their litigation[11] in the United States against the Russian based operator of the stream ripping sites *Flvto.biz* and *2conv.com* has concluded.

- *Music-Bazaar.mobi*, the download site, seems to be disabled and is no longer reported.

- *Rarbg*, the Bit Torrent website, does not seem to be available anymore.

- *Shabakaty*, a suite of apps, is no longer reported.

Actions taken by public authorities

During the public consultation, the authorities of the Republic of Korea informed the Commission of several measures they have implemented to strengthen IP protection and enforcement. The Korean Intellectual Property Office (KIPO) took proactive measures in strengthening IP enforcement in both online and offline markets, enhancing public awareness, and intensifying collaboration with international enforcement bodies. The authorities informed about the KIPO IP Police, the IP Infringement Reporting centre (an integrated one-stop platform to report IP infringements), and the Online Monitoring Team that works proactively to detect and remove counterfeit products from digital platforms. In April 2024, KIPO introduced the Multi-platform IP Guardian Reward Program, targeting vendors operating across multiple digital platforms. The authorities also described the efforts made to fight counterfeiting and piracy on physical marketplaces, such as Seomun and Dongdaemun.

Some positive developments in other countries have been reported by stakeholders and identified in the *Report on the protection and enforcement of intellectual property rights in third*

[11] UMG Recordings, Inc., et al. v. Tofig Kurbanov and DOES 1-10 d/b/a FLVTO.BIZ a/k/a 2Conv.com

countries (*Third country report*)[12]. For example, for ***China***, stakeholders reported some positive developments. They refer to a Guangzhou court decision from June 2024, which found the cloud storage service *Baidu Pan* to be indirectly liable for copyright infringement of certain TV programs, since it was negligent in failing to ensure takedown and 'stay down' of infringing copies stored on its cloud service[13]. Stakeholders also reported some positive developments in criminal enforcement in China, mentioning a criminal prosecution which led to a conviction of a notorious piracy website targeting Japanese users called *B9Good*[14], as well as criminal prosecutions against a subscription-style website called *Shenlan and Coco*[15]. The National Copyright Administration of China (NCAC) is reported to have continued to organise, in cooperation with rightsholders, the once-a-year '*Sword Net*' campaign aimed at acting against significant online services that facilitate audiovisual piracy.

In the *Annual Report on China's Combating of IPR Infringement and Counterfeiting*, from 26 April 2024, Chinese authorities report on different measures and actions related to IPR enforcement, including the special action coded '*Jianwang 2023*' to combat online IPR infringements and piracy. According to the report, this campaign took down 2.44 million links of IPR infringing and pirating content, shut down 2 390 infringing and pirating websites (APPs), and dealt with 1 513 cases of online infringement. The State Administration for Market Regulation (SAMR) is reported to have cleaned up 300 000 pieces of illegal and irregular information on various platforms and addressed unregulated live streaming. Regarding online platforms, as indicated in the *Third country report*, the SAMR has signed a cooperation agreement with 81 online platforms[16].

In ***Brazil***, stakeholders informed about positive actions in the context of *Operação 404*[17] which tackled web- and app-based piracy, including through site-blocking injunctions, as well as seizure raids against major pirate targets[18].

Stakeholders have reported improvements also in ***Thailand*** and ***India***, in particular concerning online enforcement and the site blocking process.

2. ONLINE SERVICE PROVIDERS OFFERING OR FACILITATING ACCESS TO COPYRIGHT-PROTECTED CONTENT

Online services remain the main source of copyright infringements. Various types of online service providers support access to copyright-protected content, such as music, films, books and video games, without authorisation of the rightholders. In some instances, these service providers rely on a variety of other online service providers, such as ad networks and payment services to finance their activities, hosting and caching services to support and optimise illegal distribution of content, or reverse proxy to undermine enforcement efforts. Certain online service providers also contribute directly or indirectly to copyright infringements by facilitating

[12] Published at the same time with this edition of the Watch List.
[13] Shanghai Feicui Eastern Communications Co. Ltd. v. Baidu Pan (Guangzhou Provincial Court, June 2024) (rehearing). See report at https://www.lexology.com/library/detail.aspx?g=8b979860-87e5-49da-9906-861e542f6d72
[14] *Operators of B9GOOD, one of the largest piracy sites for Japanese anime, found guilty*, published by Content Overseas Distribution Association (CODA) at https://coda-cj.jp/en/news/469/.
[15] *China's Pirate Site Crackdown is Real & Assisted By Anime Anti-Piracy Group*, published by TorrentFreak at https://torrentfreak.com/chinas-pirate-site-crackdown-is-real-assisted-by-anime-anti-piracy-group-240717/ .
[16] https://www.samr.gov.cn/zfjcj/sjdt/gzdt/art/2024/art_bb250c0edaa64d29acb7d23b91b10974.html
[17] https://agenciabrasil.ebc.com.br/tags/operacao-404
[18] https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-404-chega-a-4a-edicao-com-buscas-no-metaverso-suspensao-de-4-canais-e-90-videos-retirados-do-ar

access to unauthorised content made available by third parties or providing devices and products or services to circumvent technological protection measures used by rightholders to prevent or restrict unauthorised acts.

As the technological and business landscape evolves, presenting new and innovative methods and technologies for marketing products or distributing content, so does the online counterfeit and piracy landscape. IP infringers swiftly adopt new technologies as part of their illicit activities to target consumers and circumvent IP enforcement efforts by rightholders and law enforcement authorities.

3.1 Trends, new services and practices in online piracy

As part of this edition of the Watch List, contributors were invited to provide information on the latest trends in online IP infringements. The identification of such trends allows to reflect in the Watch List different forms of IP threats that may require attention from relevant intermediary services and governments outside of the EU.

(i) Use of apps in the context of IP infringing activities[19]

The number of applications (apps) has grown rapidly over the past decade, with usages expanding from mobile devices to all connected devices, such as smart TVs and watches. Apps are now a major way for users to access various online services and content. While this development has provided many benefits for consumers and businesses, it has also led to its misuse to conduct illegal and fraudulent activities, including IP-infringing activities.

Some contributions pointed to piracy apps, which support illegal copying or distribution of copyright protected content, such as music, movies, series or books, as the most prevalent emerging digital piracy method[20]. Some apps also infringe IP rights by using a company's trademark or logo to deceive users into thinking the app is legitimate. This tactic misleads users into using fraudulent apps selling counterfeit products or spreading malware.

IP infringers are using various methods to avoid detection of illegal activities by app stores, rightholders and enforcement authorities. This includes apps that appear as games or other legitimate apps to conceal their purposes. Some piracy apps have integrated Virtual Private Networks (VPNs) to hide their users' IP addresses and bypass blocks or geolocation restrictions. Another challenge is that even if an app is taken down from an app store, it remains usable on the devices on which it has already been installed. Additionally, the increasing number of app stores, as well as sources outside app stores where apps can be downloaded, expands the number of online services that must be monitored and notified for IP infringing apps. This includes social media and forums where links to download apps are shared, as well as hosting providers that may not answer any takedown requests.

Legitimate apps can also be used in support of IP-infringing activities. This is notably the case of social media and messaging apps that are used to promote, share information and/or facilitate transactions related to such activities. Some contributions also pointed to the growing concerns with some social media apps providing file sharing or streaming functionalities which are used

[19] EUIPO, Discussion paper, *APPS & APP STORES - Challenges and good practices to prevent the use of apps and app stores for IP infringement activities*, Alicante, 2024, https://data.europa.eu/doi/10.2814/788692.
[20] INTERPOL, *Digital Piracy Methods, Project I-SOP, Online crimes targeting consumers governments and creative industries*, 2023, https://www.interpol.int/en/Crimes/Illicit-goods/Project-I-SOP.

to share pirated content in closed groups of users that can have hundreds of thousands of members.

(ii) IPTV piracy services

Internet protocol television (IPTV) piracy involves illegal streaming of TV, films, series, live sports and other type of events over Internet Protocol networks, sometimes mimicking legitimate IPTV services. These pirate services can bring content to multiple displays, including TV screens, with subscriptions or ads-based business models. It can also be downloaded to a consumer device (i.e. a receiver) subsequently connected to a TV set to enable it to stream the content. Moreover, stakeholders report that some consumer devices are sold with one or more pre-installed pirate IPTV applications. The business model of unlicensed IPTV services is usually based on subscriptions. Many consumers may actually be unaware that these Pay-TV services are illegal.

IPTV piracy inflicts significant economic damage, including revenue losses for content creators and service providers, reducing the value of broadcast rights, and increasing the need for costly anti-piracy measures. Stakeholders report that illegal IPTV is the most serious threat for the audiovisual rightholders. They refer to the EUIPO report from September 2023 that concludes that 58% of online piracy is streaming (IPTV) and 32% downloading[21].

Monitoring the activities of unlicensed IPTV services is particularly difficult. As explained in the section on piracy apps above, some unlicensed IPTV services make their apps available in 'unofficial' app stores or websites[22], which do not have a procedure in place to notify apps that infringe copyright. Others invite their users to download generic apps (i.e. generic video players, not illegal as such) and explain to them how to use those apps to stream the infringing content that the unlicensed IPTV services provide[23].

There are likely to be thousands of pirate IPTV apps and services in the world. The pirate IPTV landscape is complex and difficult to penetrate because it typically involves multiple layers of restreaming and reselling. At the root of the problem lie the pirates who copy the television channels and video-on-demand (VOD) content at source. Often these pirates will be very technically sophisticated and engage in various types of hacking to evade and circumvent copy controls and other anti-streaming technologies. The pirated content is then aggregated with other channels and content, and supplied on to other IPTV services, in a complex web of restreaming. Much of this restreaming is facilitated using middleware which makes it relatively easy to administer and operate a pirate IPTV service. Many pirates also 'pirate' from each other, further adding to the complexity of the landscape.

This complex network of copying, reselling, exchanging and restreaming broadcasters' content constitutes a parallel black market that explains the multiplication of a single stream of a TV channel, eventually available not only in hundreds of unlicensed IPTV services but also in illegal streaming websites and online content-sharing service providers. Moreover, this complex

[21] EUIPO, *Online copyright infringement in the European Union: films, music, publications, software and tv (2017-2022)*, Alicante, 2023, https://data.europa.eu/doi/10.2814/966644.
[22] These refer to other app stores than Google Play, Apple Store, or other mainstream app stores.
[23] Stakeholders from the audiovisual and broadcasting sectors have reported some of these generic applications for inclusion in this Watch List. However, none of them is listed in this document, as the evidence provided shows that they are mere video players, even if they are used by some unlicensed IPTV operators to infringe copyright.

network is the result of cooperation of illegal operators from various countries, making it difficult to find out the identity and precise location of an IPTV operator.

Stakeholders report that IPTV services have been the driving force in the emergence of a number of related illegal businesses including the ones engaged in (i) the resale of IPTV services, (ii) individuals or businesses involved in the theft, distribution, and sale of channels, and (iii) manufacturers of set-top-boxes, illegal streaming devices (ISDs). IPTV services must rely on infrastructure and support services to function, such as hosting providers, media servers, and panel hosting. Some of these services are used without the knowledge or approval of the legitimate provider of service or product. However, others intentionally tailor their business strategy towards illegal sites or ignore bad actors amongst their clients even when informed of their illegal activities.

The marketing and sale of IPTV services is often carried out by a growing network of global IPTV service resellers who purchase subscriptions at wholesale prices and resell them for a profit, further complicating investigations. These resellers are also often involved in the promotion and support of the service with many also providing a limited number of channels to a given service. It is not uncommon to see resellers expand on their business model and move on to become an illegal IPTV service provider.

While assessing the exact scale of IPTV piracy remains a challenge, the outcome of the most recent EU law enforcement operations, leading to the closure of IPTV services with millions of users [24] demonstrates the scale of such illegal services. Enforcement against such services is challenging due to their technical sophistication, consumer demand for cheap content, but also jurisdictional issues. Stakeholder contributions pointed to the fact that even though such services are legally located outside of the EU, they target EU users and rely on technical infrastructure located in the EU to optimise the quality of their illegal content distribution.

Some stakeholders reported that illegal IPTV subscriptions are advertised and sold on social media platforms, as well as e-commerce platforms. They also indicated that devices to be plugged on TV screens (HDMI dongles) with pre-installed apps to access illegal IPTV services are sold on some online marketplaces.

(iii) Live event piracy

The main value of live events lies in the exploitation of their live performance, making live event piracy particularly damaging. Live event piracy raises new challenges for rightholders, online intermediaries, law enforcement and judicial authorities alike, as limiting its damages requires prompt action to interrupt the illicit live streams.

Several contributions are pointing to the development of live event piracy through IPTV services and apps, as well as web stream services, that can be subscription or ads based. The operators of such services often use hosting providers registered in countries outside of the EU with lenient regulation regarding their activities while using technical infrastructure located in the EU to optimise content delivery. Some contributions explain that this presents significant challenges for rightholders, as some operators located outside of the EU do not respond to take-down

[24] News item: https://www.europol.europa.eu/media-press/newsroom/news/european-law-enforcement-stops-illegal-iptv-service-providers.

requests. In some cases, these operators advertise their services as 'bullet-proof' hosting, indicating they do not answer such requests or provide information about their users.

(iv) Interplanetary File System

The Interplanetary File System (IPFS) is a distributed file storage system that enables the decentralised storage and sharing of content in a peer-to-peer manner, similar to BitTorrent. In this system, users act as nodes of the network, hosting and serving files and websites, each holding a portion of the overall data. IPFS provides a decentralised infrastructure that supports the development of various applications, including those based on blockchain technology. Unlike the World Wide Web, which relies on location-based addressing using URLs, IPFS employs content-based addressing using content identifiers (CIDs), which are hashes[25] of the content itself.

Internet users access content stored on IPFS in two main ways: either by installing an IPFS client software to become a node in the network or by utilising public or private IPFS gateways. Public gateways are openly accessible to everyone. IPFS gateways serve as a bridge between the IPFS network and applications that do not natively support the IPFS protocol and rely on standard web protocols like HTTP, such as web browsers. By allowing the use of standard web protocols, gateways facilitate easier access to IPFS-stored content for a broader audience.

The decentralised and global nature of IPFS makes tracking of the origin of infringing content difficult and limits takedown efforts. However, gateway operators can voluntarily implement content filtering measures, such as using lists of CIDs to block. Some stakeholders in the publishing industry have reported that services like *Library Genesis* (*LibGen*), *Z-Library*, and *Anna's Archive* utilise IPFS to illegally distribute copyright protected content, including through public gateways.

(v) Other trends

Besides these more general trends some new problematic practices and services have been reported. For example, related to Artificial Intelligence (AI), stakeholders in the music sector report concerns with the vocal cloning services that enable users to create 'deep fake' tracks where an AI generated version of an artist's voice is set against a new composition and AI vocal clone covers. The process of vocal cloning may involve multiple acts of unauthorised reproductions. These services can be offered in the form of websites, bots and apps have proliferated. Rightholders from different sectors report concerns about illegal datasets for training generative AI large language models (LLMs) with copied content from illegal sources.

Music industry also reported streaming manipulation services supporting royalty fraud, such as *Justanotherpanel.com* (JAP), a Russian-based streaming manipulation service, which offers, for a fee, the generation of artificial streams or 'plays' on digital service providers, such as Spotify, Soundcloud, Apple Music, Amazon Music, Tidal and YouTube, with various packages available for purchase. By generating artificial streams of their content, fraudsters are diverting a portion of the royalties that should be paid to genuine creators. The music industry reported the use of AI by fraudsters to generate content made available on digital service providers, as well as by

[25] Hashing is a process of using a mathematical algorithm against data to produce a numeric value that is representative of that data, https://csrc.nist.gov/glossary/term/hashing.

streaming manipulation services to fake users' engagement and undermine the stream manipulation detection measures put in place by digital service providers.

Registrars and registries have been reported again as they play a crucial role in the online piracy eco-system. They are uniquely positioned to take action to stop and suspend or terminate domain names used by websites infringing IP. Some examples of mentioned registrars include *Namecheap, Pananames, PDR Ltd. d/b/a PublicDomainRegistry.com, Tucows, Tonic Registry* and *Me Registry*.

The pharmaceutical industry reported *NiceNic International Group* domain registrar which allegedly hosts an outsized portion of rogue pharmacy websites (estimated at around14% of all rogue pharmacies as of last year). Furthermore, despite maintaining ICANN accreditation, BrandShield estimates that they remove as little as 20% of the problematic domain names reported to them.

Stakeholders in the audiovisual sector reported a number of television operators, which illegally broadcast movie or television titles, purchased on DVD or illegally obtained otherwise (e.g. downloaded from pirate websites). TV channels can also be illegally rebroadcasted by redistributing the signal originating from a single subscription, or directly from satellite networks.

The video game industry reported some negative developments in three main areas: (i) the use of malware in illegal game downloads, (ii) the prevalence of cryptocurrency for illicit game sharing, and (iii) scene release groups that use various methods to allow for more widespread, faster illegal game downloads. Scene release groups facilitate commercial scale piracy by circumventing technological protection measures and packaging' illegal downloads to be more easily accessed and used by the general public.

Rightholders in the video games industry also reported unauthorised sales of in-game digital items and 'cheat' software products[26]. They list a number of sites that provide 'cheats', which can infringe IPR in instances where the cheat software code copies the underlying code of the game software, for example *se7ensins.com, unknowncheats.me*. They also refer to online sites that provide a platform for users to list and sell unauthorised digital items including in-game currency, in-game items, game accounts, and the unlicensed sale of potentially fraudulent game keys, which can provide access to features within a game or to the game itself, for example, *playerauctions.com, G2G.com.*

Rightholders in the sports events industry reported *Control Word Sharing* piracy, also known as *Internet Key Sharing (IKS)* - a form of piracy that impacts pay TV broadcasters, mainly on satellite. It consists of hacking the content protection in one device and distribute on the Internet encryption keys, known as control words, to users equipped with rogue receivers. They also reported some branded media devices associated with piracy and sold across the globe, such as *Zhuhai Gotech Intelligent Technology Co., Ltd.* The devices are typically sold preloaded with pirate firmware: control word sharing software and illicit IPTV services. *Icone* is another example mentioned, that can turn a range of consumer electronics goods, including media devices and television into receivers. They are typically supplied preloaded with apps that enable control word sharing such as *Orca IKS*, as well as pirate IPTV apps – in particular *GoGo* IPTV.

[26] These products enable an unfair and rapid collection and aggregation of virtual goods, such as bots, hacks and cheats, or which otherwise tilt the scales in favour of one player over another.

3.2 Service providers that offer content protected by copyright and service providers that directly or indirectly facilitate access to this content

The following section lists service providers that offer content protected by copyright and service providers that directly or indirectly facilitate access to this content. Some of the mentioned service providers were reported because they do not apply practices that prevent or substantially reduce the risk of their services being used for the purposes of infringing copyright. The service providers are grouped in sub-sections according to their business model and type of service they provide, following a structure similar to the one used in the previous editions of the Watch List.

3.2.1 Cyberlockers

A cyberlocker is a type of cloud storage and cloud sharing service that enables users to upload, store and share content in centralised online servers. Content stored in cyberlockers may be protected by copyright or not. However, if a user uploads copyright-protected content and shares the URL link, others can download that content without the authorisation of rightholders. Moreover, the URL links to the infringing content are usually promoted across the internet by different means, such as social media platforms, blogs, emails, mobile applications or links in other websites, including linking and referring sites (see Section 3.2.3 below).

Stakeholders continue to report cyberlockers as a major piracy threat and refer to the different ways used by cyberlockers listed in this section to facilitate wider distribution of illegal content, including unauthorised/leaked pre-releases of content, which creates high economic harm for rightholders. They also continue reporting difficulties to take action against those services due to the often-masked ownership information. Stakeholders ***from various creative industries*** have reported that the cyberlockers listed below received notices to take down content or cease and desist letters, but they did not react or did not remove the content, even if some of them publish their IP policies.

Mega.nz/.io

Mega was reported for inclusion in the Watch List by stakeholders in ***the music industry***. They report that *Mega.nz* is a popular site used by respondents for downloading infringing music, including pre-release content. They also report on some action by law enforcement authorities and civil litigation against *Mega* initiated by the rightholders in the film and recorded music industries. Rightholders report that more recently, M*ega* is used to host AI vocal models.

The stakeholders report *Mega* for the lack of preventive measures to avoid uploads of infringing content. According to their information, in January 2022, internet service providers (ISPs) in Russia were ordered to permanently block the site following music rightholders' actions.

Mega.nz had a global SimilarWeb ranking of 337, industry ranking (file sharing and hosting) of 4 and received 87.01 million visits globally in February 2025.

Rapidgator - rapidgator.net

Stakeholders across ***different sectors, including publishing, music and audiovisual***, continue reporting *Rapidgator* for inclusion in this Watch List. *Rapidgator* is reported to play a key role in the music piracy ecosystem, specifically in relation to the making available of pre-release music content. According to data from the rigthholders, almost 100 000 files infringing copyright (movies, series, documentaries) have been detected between January and June 2024. As reported in 2020, Russian courts issued a blocking injunction against *Rapidgator* in 2019[27]. However, the site is still accessible from other countries. Legal action concerning *Rapidgator* also includes decisions issued in Germany[28].

Rapidgator is reported to comply with takedown notices, but it allegedly makes no effort to remove other uploads of the same infringing content or to prevent infringing content from being re-uploaded immediately after the takedown. Publishers report that this cyberlocker has been sent hundreds of thousands of takedown requests and remains a significant source of infringement although there has been an increase in compliance with the requests.

Rapidgator had a global SimilarWeb ranking of 2 038, industry ranking (file sharing and hosting) of 16 and received over 25,45 million visits globally in February 2025.

Dbree - dbree.org

The ***music industry*** has again reported *Dbree* for inclusion in the Watch List. This cyberlocker is reported to be detrimental towards the music industry due to its use in connection with the distribution of pre-release content. Links to infringing content hosted on *Dbree.org* are reported to be frequently found on known leak sites and forums. The operator(s) of *Dbree.org* take several steps to try to hide their identities. The service is reported by stakeholders to be unresponsive to infringement notices. In November 2021, the Italian Regulatory Authority for Communications (AGCOM) ordered ISPs to block access to *Dbree.org*. According to music industry's information, the site has also been subject to blocking orders in France[29], Spain[30] and Brazil[31].

Dbree had a global SimilarWeb ranking of 82 477, industry ranking (music) of 857 and received 427 791 visits globally in February 2025.

Doodstream

Doodstream was reported by ***audiovisual rightholders*** for inclusion in the Watch List as one of the largest illegal video hosting services in the world. It pays users to upload popular (including copyright protected) content onto *Doodstream*, which could then be disseminated through weblinks on illegal streaming websites and other platforms. It is reported to have implemented various tools to allow its uploaders to evade takedown and enforcement efforts.

In March 2024, a group of plaintiffs filed a lawsuit against *Doodstream* in the Delhi High Court[32]. In May 2024, the Court granted an interim injunction against the operators of

[27] Moscow City Court Appeal Ruling 33/150 of 23 January 2019.
[28] District Court of Hamburg, decision 308 O 224/18 of 12 July 2018 and decision 310 O 193/19 of 23 July 2019.
[29] Décision du 25 Janvier 2022 3ème chambre 3ème section N° RG 21/14912 - N° Portalis 352J-W-B7F-CVVOR and Décision du 11 janvier 2024 3ème chambre 1ère section N° RG 23/14793 N° Portalis 352J-W-B7H-C3J6Y.
[30] Auto nr. 26/24 of 27 February 2024.
[31] Officio nº 12082240/2023 – CYBERGAECO, 27 November 2023.
[32] Delhi High Court, Warner Bros. Entertainment Inc. & Ors. v. Doodstream.com & Ors, 13 May 2024.

Doodstream, though the domains are still active, and the defendants have failed to comply with the court's orders. Various *Doodstream* domains have been blocked in France[33].

Doodstream had a global SimilarWeb ranking of 34 226, industry ranking (web hosting and domain name) of 156 and received 2.141 million visits globally in February 2025.

Z-Library

Z-library was reported by ***book publishers*** for inclusion in the Watch List as a network of infringing sites that focus specifically on sharing books and journal articles. The site's e-book section claims to be the world's largest e-book library', while it is described on its academic articles page as 'the largest collection of scientific articles in the world'. The network of sites frequently moves between domains. Despite a series of law enforcement actions since November 2022, with the removal of hundreds of infringing *Z-Library* domains and the arrest of two site operators[34], the network is reported to still engage in pirate activities via multiple domains and have still three websites active.

*Z-library.rs*had a global SimilarWeb ranking of 25 303, industry ranking (education) of 9 057 and received 193 989 million visits globally in February 2025.

3.2.2 Stream-ripping services

Stream-ripping services are websites, software and apps that enable users to obtain a permanent copy of audio or audiovisual content by downloading it from online streaming platforms[35]. Stream-ripping services enable users to copy the URL of content taken from a streaming platform and paste it into a search box on the stream-ripping site. The stream-ripping site converts the content and creates a media file. According to the relevant rightholders, this operation usually involves the circumvention of the technological protection measures applied by the streaming platforms. Stream-ripping services often provide a search function on their platform, so that the user does not need to search for a link on other platforms.

Stakeholders report that advertising is the main revenue source of stream-rippers, with many disseminating malware to obtain the users' personal data or bank payment details. According to stakeholders, stream-rippers are causing significant losses for the ***music, film and television industries*** by having a negative impact on the income from legal streaming services and sales from the legal download services.

According to the input from the music industry, stream ripping services continue to be the biggest piracy problem, which according to the estimate of the International Federation of the Phonographic Industry (IFPI) account for 600 million illegal downloads in the 12 months up to June 2024. IFPI's study of 2023[36], the largest music-focused consumer study worldwide, found

[33] Court of Paris, National Federation of Film Editors and Ors. v. SA Société Françoise du Radiotelephone and Ors., 6 July 2023.
[34] Criminal prosecution in the United States, which resulted in the arrest of two alleged operators in Argentina. The FBI have seized hundreds of domain names belonging to the site. In parallel, following a legal action by the French Publishers Association against Z-Library, in 2022, the French judicial court ordered ISPs to block a large number of domain names providing access to this website.
[35] These online streaming platforms may be legal operators that have acquired licences for streaming content. Stream-ripping services allow users of such platforms to download to their devices content that otherwise would only be available through streaming.
[36] https://www.ifpi.org/wp-content/uploads/2023/12/IFPI-Engaging-With-Music-2023_full-report.pdf

stream ripping to be the key music piracy threat. The study was conducted in 26 countries gathering the views of 43 000 respondents. The study found that 26% of respondents had used stream ripping sites as a way to listen to or obtain music.

YTMP3.CC, Ytmp3.nu

Ytmp3.cc has been reported by rightholders in ***the music industry*** as a stream ripping service where users can convert and download video and audio content from various platforms. As a result of the legal action taken by RettighedsAlliancen on behalf of Danish music rightholders, court-issued orders were obtained for the blocking of access to *Ytmp3.cc* as of March 2023. Following music rightholders' actions, *ytmp3.nu* is currently subject to website blocking orders also in Brazil[37] and Spain[38].

Ytmp3.cc had a SimilarWeb global ranking of 11 341, industry ranking (music) of 119 and received 5 765 million visits globally in February 2025.

Ytmp3.nu had a SimilarWeb global ranking of 54 486, industry ranking (music) of 927 and received 1.586 million visits globally in February 2025.

Y2mate.com and related sites, including YT1s.com, https://www-y2mate.com/, https://en.y2mate.is

Stakeholders from ***the music industry*** continue reporting *Y2mate* for inclusion in this Watch List. On *Y2mate* users are able to convert and download either an audio-only MP3 file or the entire audiovisual work as an MP4 file through the site. Following music rightholders' actions, *Y2mate* is reported to be currently subject to website blocking orders in 11 countries, including Argentina[39], Brazil[40], Denmark[41], Ecuador[42], India[43], Indonesia[44], Italy[45],Peru[46], Mexico[47] and Spain[48]. Previously the operator voluntarily geo-blocked *Y2mate.com* from the US, the UK, Germany and France but these restrictions are reported not to be in place any longer. Rightholders report that the operator is running other stream ripping sites including *YT1s.com* and *9convert.com*.

---

[37] Tribunal de Justiça do Estado de São Paulo, Decisão nº 1018314-89.2021.8.26.0050, 10 August 2021.
[38] JDO. CENTRAL CONT/ADMVO. N. 8, AUTO nº 95/2023, 31 October 2023.
[39] Poder Judicial de la Nación, Juzgado Civil 29, Nr. 79823/2022, 25 October 2022.
[40] On 10 August 2021, the Tribunal of Justice of the State of São Paulo, issued a permanent blocking order against 14 stream-ripping sites including Y2mate.com, Flvto.biz and 2conv.com following an application filed by the Prosecutor's Office Anti-Organized Crime Group (CYBER GAECO), the Prosecutor's Office of the State of São Paulo (DEIC) and APDIF DO BRASIL (the recording industry anti-piracy association).
[41] Retten I Næstved Retsbog, Sag BS-6391/2023-NAE, 13 March 2023.
[42] On 23 July 2021, SENADI (the Ecuadorian Intellectual Property Office) ordered ISPs to block access to four stream ripping websites including Y2mate.com following an application by SOPROFON (the music industry's collective management organisation in Ecuador).
[43] High Court of Delhi at New Delhi, CS(COMM) 13/2023, Order of 28 May 2024 I.A. 30731/2024.
[44] According to media, the Indonesian government started blocking illegal sites in the middle of 2019 and by April 2022 the total number of sites blocked in Indonesia had topped 3,500, see: https://www.advanced-television.com/2022/04/11/indonesia-claims-site-blocking-success/ .
[45] Italian Regulatory Authority for Communications (AGCOM), Order 70/19DDA of 13 February 2019, https://www.agcom.it/provvedimenti/determina-70-19-dda.
[46] According to the copy of INCOPI comments under the US Special 301 Report, as published by torrentfreak.com at https://torrentfreak.com/images/peru-301.pdf.
[47] The site was blocked via the administrative blocking procedure in place and ISPs were notified via a letter from the Mexican Institute of Industrial Property (IMPI) to block the site.
[48] Juzgado de lo Mercantil nº 8 de Barcelona, sentencia nº 27/2020.

Y2mate.com had a global SimilarWeb ranking of 1 715, industry (search engines) ranking of 58 and received 24,93 million visits globally in February 2025.

X2mate.com

Stakeholders from ***the music industry*** reported *X2mate.com* for inclusion in this Watch List. The site explains to users how to download YouTube videos. The site operator and the location of the operator is currently unknown. The site is subject to website blocking orders in Brazil[49] and Peru[50].

X2mate had a global SimilarWeb ranking of 700 892, industry (music) ranking of 8 491 and received 59,917 million visits globally in February 2025.

Savefrom - Savefrom.net /ssyoutube.com/sfrom.ne, sfrom.ne and mirror sites

Stakeholders from ***the music industry*** continue reporting *Savefrom* for inclusion in this Watch List. *Savefrom* circumvents the YouTube content protection measures and serves up the unprotected content to users directly from the YouTube servers from where the user can either save the video or save the audio to their devices. It is reported that in April 2020, the service announced that it would be discontinuing its offer in the US, in the UK and Spain. However, the service continues to operate in other territories. *Ssyoutube.com* is being run by the same operator as *Savefrom.net*. Following music rightholders' actions, *Savefrom.net* is currently subject to website blocking orders in Brazil[51], Denmark[52], India[53] and Spain[54] and *ssyoutube.com* is blocked in Brazil[55] and Spain[56].

Savefrom had a global SimilarWeb ranking of 358, industry (file sharing and hosting) ranking of 5 and received 112.5 million visits globally in February 2025.

3.2.3 Linking or referring websites

Linking or referring websites aggregate, categorise, organise and index links to content that is usually stored on other sites allegedly containing pirated content, including cyberlockers and hosting sites. Linking to third-party sites reduces their maintenance costs. Others, however, host the content files on servers they control.

Linking sites offer search tools and often categorise and organise the content by title, album, genre or, in the case of TV series, season. The users obtain detailed information on the content and can choose to download or stream a film file or a music track or album by being redirected

[49] Tribunal de Justiça do Estado de São Paulo, Decisão nº 1023912-87.2022.8.26.0050, 24 March 2023.
[50] Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), Resolución n° 0479-2023/CDA-INDECOPI, 20 December 2023.
[51] Tribunal de Justiça do Estado de São Paulo, Decisão nº 1023912-87.2022.8.26.0050, 24 March 2023.
[52] Retten I Næstved Retsbog, Sag BS-6391/2023-NAE, 13 March 2023.
[53] High Court of Delhi at New Delhi, CS(COMM) 13/2023, Order of 28 May 2024 I.A. 30731/2024.
[54] On 7 May 2021 the Mercantile Court of Barcelona ordered ISPs to block multiple stream-ripping websites including Savefrom.net following an application by submitted by AGEDI (the music industry's local collecting society). Juzgado de lo Mercantil nº 02 de Barcelona, Procedimiento ordinario (Materia mercantil art. 249.1.4) - 1824/2020 –P.
[55] Tribunal de Justiça do Estado de São Paulo, Decisão nº 1023912-87.2022.8.26.0050, 24 March 2023.
[56] See footnote 53.

to another site, from where the download or streaming starts automatically. Alternatively, the streaming of the content occurs directly on the same website. In this case, instead of providing a text hyperlink, the site may embed or frame the content to stream it in a video player. Some sites also combine lists of links with video players. The linking or referring sites listed below pursue financial gains through income from advertising and referrals.

The music and film industries are particularly concerned, since, allegedly, linking sites often make available pre-release content.

Fmovies- https://fmoviesto.site/, https://f-moviesz.to

Fmovies continued to be reported by ***audiovisual industry*** for inclusion in the Watch List. It is reported to be one of the most popular websites in the world for streaming pirated copies of popular movies and television shows and having more than 60 associated domains used by significant piracy operations such as *Bmovies, 9anime, Putlocker, and Solarmovies* and, likely sources files from the streaming piracy service.

Fmovies domains are subject to site blocking orders in at least 16 jurisdictions, including India[57], Australia[58], Denmark[59], Indonesia[60], Malaysia[61], and Singapore[62]. At the time of writing, a number of domains associated with the syndicate, including the main *Fmovies* domains, *fmovies24.to, fmoviesz.to,* and *fmovies.to,* as well as the video library *vidsrc[.]*appear to have been taken offline.

Fmovies.to had a global SimilarWeb ranking of 36 808, industry (TV, movies and streaming) ranking of and received 2.738 million visits globally in February 2025.

Seasonvar - Seasonvar.ru

Stakeholders from ***the audiovisual industry*** continued reporting *Seasonvar.ru* for inclusion in this Watch List. *Seasonvar* is a Russian-language streaming website that offers free access or a premium subscription that allows users to download or stream HD audiovisual content without any advertising interruptions. On its website it claims to have 288 722 series[63]. The website is allegedly hosted in Russia. Legal action concerning this site includes blocking orders in Russia[64] and Spain[65].

Seasonvar had a global SimilarWeb ranking of 7 125, industry rank (TV movies and Streaming) of 303 and received 10.9 million visits globally in February 2025.

Rlsbb - Rlsbb.ru

[57] Delhi High Court, UTV Software Communication LTD and Ors. v. 1337X.TO and Ors., 24 October 2019.
[58] Roadshow Films Pty Ltd v Telstra Corporation Limited [2017] FCA 965, NSD269/2017, 18 August 2017.
[59] District Court Frederiksberg, Rights Alliance Denmark v. TELENOR, 9 February 2017; District Court Frederiksberg, Rights Alliance Denmark v. TDC, 8 January 2019.
[60] Decision of the Directorate General of Intellectual Property Rights (DGIPR), 20 December 2017.
[61] First blocked through an executive order in 2017.
[62] Disney Enterprises Inc. v. M1 Limited, HC/OS 95/2018, 26 April 2018.
[63] Status on 14 March 2025.
[64] Moscow City Court, civil case No. 3-1127/2018, 24 December 2018.
[65] Juzgado de lo Mercantil nº 9 de Barcelona, sentencia nº 159/2020, 6 July 2020.

Stakeholders from ***the audiovisual industry*** have again reported Rlsbb for inclusion in the Watch List. The English-language website allegedly facilitates access to a wide range of infringing content by regularly posting articles that contain details about movies and other types of content, together with links to cyberlockers. As reported in previous editions of the Watch List, legal action concerning this website includes blocking orders in Belgium[66], Denmark[67], Italy[68] and Portugal[69], Malaysia[70], United Kingdom[71], Indonesia[72], and Australia[73].

Rlsbb had a global SimilarWeb ranking of 18 694, industry ranking (arts and entertainment) of 226 and received 2.710 million visits globally in February 2025.

Rezka.ag

Stakeholders from ***the audiovisual industry*** have reported *Rezka* again for inclusion in the Watch List. *Rezka* is a popular Russian-language streaming website that allegedly offers 31 000 movies and 8 800 TV series, as well as cartoons and anime. The site has been subject to blocking orders in Russia[74], Spain[75], Malaysia[76], Brazil[77], Australia[78], Indonesia[79] and Lithuania[80].

Rezka.ag had a global SimilarWeb ranking of 1 743, industry ranking (TV movies and streaming) of 84 and received 40.12 million visits globally in February 2025.

Dytt8[.]net, Dytt89.com, Dy2018.net, Dy2018[.]com, Dydytt[.]net, and Ygdy8[.]com

Dytt8[.]net was reported by ***the audiovisual industry*** for inclusion in the Watch List. The website provides direct links to third-party storage providers and is part of a group of related sites including *dytt89[.]com, dy2018[.]com, dy2018[.]net, dydytt[.]net*, and *ygdy8[.]com*. As reported, the sites were referred to the National Copyright Administration of China (NCAC) in 2019 and 2022 as part of its annual 'Swordnet' campaign. *Dytt8.net* is blocked in Australia[81] and Malaysia[82] and *Dy2018.com* is blocked in Malaysia[83].

[66] Jugement du Tribunal de commerce francophone de Bruxelles, rép. 004235; A/18/00217, 30 March 2018.
[67] Retten I Holbæk Retsbog, BS-13084/2018-HBK, 28 May 2018.
[68] Italian Regulatory Authority for Communications (AGCOM), Order n. 177/DDA/CA, reaffirmed by decision n. 20/15/PRES, 20 July 201, https://www.agcom.it/provvedimenti/presidenziale-20-15-pres.
[69] IGAC, 28 December 2015, pursuant to a Memorandum of Understanding: Análise de queixa formulada à IGAC ao abrigo da Cláusula 5ª do Memorando de Entendimento celebrado em 30 de julho de 2015.
[70] First blocked through an executive order in 2017.
[71] High Court London, Columbia Pictures Industries Inc and Ors. v. British Telecommunications PLC and Ors., 3 February 2022.
[72] Decision of the Directorate General of Intellectual Property Rights (DGIPR), 30 May 2018.
[73] Roadshow Films Pty Ltd v Telstra Corporation Limited [2017] FCA 965, NSD269/2017, 18 August 2017.
[74] Decision of the Ministry of Communications and Mass Media, 1z-7605/2019, 5 August 2019.
[75] Juzgado de lo Mercantil nº 9 de Barcelona, sentencia nº 159/2020, 6 July 2020.
[76] Ministry of Domestic Trade Co-operatives and Consumerism (MDTCC), 27 July 2023.
[77] Criminal District Court Sao Paulo, 7 July 2021.
[78] Roadshow Films Pty Ltd v Telstra Corporation Limited, NSD803/2020, 28 September 2020.
[79] Decision of the Directorate General of Intellectual Property Rights (DGIPR), 21 February 2020.
[80] Lithuanian Radio and Television Commission, KS-23, 26 February 2020, sanctioned by Administrative Court ruling in an administrative case No. eI2-2579-463/2020, 28 February 2020.
[81] Roadshow Films Pty Ltd v Telstra Corporation Limited [2020] FCA 507, NSD1940/2019, 20 April 2020.
[82] Ministry of Domestic Trade Co-operatives and Consumerism (MDTCC), 15 November 2019.
[83] Ibid.

Dytt89.com had a global SimilarWeb ranking of 22 016, industry ranking (social networks and online communication) of 281, and 2 449 million visits in February 2025.

Hianime (formerly Aniwatch[.]to and zoro[.]to)

Stakeholders from ***the audiovisual industry*** have reported *Hianime* for inclusion in the Watch List. *Hianime* is reported to be one of the most popular pirate streaming sites globally, and understood to be a rebrand of the previously popular sites, *aniwatch[.]to* and *zoro[.]to*. The website provides pirated versions of popular movies and television, particularly anime.

Hianime had a global SimilarWeb ranking of 102, industry ranking (TV movies and streaming) of 4 and received 339.4 million visits globally in February 2025.

Cuevana[.]biz and Cuevana3[.]eu, Cuevana3[.]ch, Cuevana.is

Stakeholders from ***the audiovisual industry*** have reported *Cuevana* for inclusion in the Watch List. *Cuevana[.]biz* is a popular streaming site amongst the Spanish speakers that offers a large library of titles including movies and TV shows. *Cuevana.biz* and *Cuevana3.eu* are currently blocked in Spain[84].

Cuevana.is had a global SimilarWeb ranking of 1 423, industry rank (TV movies and streaming) of 68 and received 36.51 million visits globally in February 2025.

Cuevana.biz had a global SimilarWeb ranking of 2 589, industry rank (TV movies and streaming) of 117 and received 15.76 million visits globally in February 2025.

nsw2u.xyz/nsw2u.com/nsw2u.net

Stakeholders in ***the video game industry*** have reported *nsw2u.xyz/nsw2u.com/nsw2u.net* for inclusion in the Watch List. The websites are reported to index, manage and organise links to unauthorised copies of games hosted on third-party platforms. Operators of these domains are reported not to have reacted to requests by rightholders to end the illegal activities. A website-blocking injunction has been issued by the UK High Court under which the UK's main internet access providers were ordered to block their subscribers' access to *nsw2u.xyz, nsw2u.com* and the related domains *nsw2u.org, nsw2u.net* and *nswrom.com*. *Nsw2u.xyz* and *nsw2u.com* were also blocked in Spain[85] and Portugal[86] following voluntary protocols with local ISPs supervised by the Spanish Ministry of Culture and the Portuguese General Inspection of Cultural Activities (IGAC), respectively. In Italy[87], the same websites have been blocked through administrative

[84] Commercial Court Barcelona, Warner Bros. Enternainment Inc and Ors. v. Orange Espagne S.A.U. and Ors., 27 October 2020; Commercial Court Barcelona, Netflix Inc and Ors. v. Euskaltel S.A and Ors., 27 September 2021; Commercial Court Barcelona, Warner Bros. Enternainment Inc and Ors. v. Orange Espagne S.A.U. and Ors., 21 December 2022; Commercial Court Barcelona, Disney Enterprises, Inc and Ors. v. Orange Espagne S.A.U. and Ors., 6 July 2020; Commercial Court Barcelona, Universal City Studios LLLP and Ors. v. Orange Espagne S.A.U. and Ors., 10 July 2019.

[85] https://www.cultura.gob.es/dam/jcr:a4a9c334-3208-4753-807a-7424e8629a7d/boletin-seccion-segunda-cpi-es.pdf.

[86] News item: https://torrentfreak.com/nintendo-wins-high-court-injunction-to-block-access-to-pirated-switch-roms-211224/.

[87] Ibid.

proceedings by AGCOM, the Italian Regulatory Authority for Communications. *Nsw2u* sites have also been blocked in both Germany[88] and France[89].

Nsw2u.com had a global SimilarWeb ranking of 17 721, industry ranking (video games consoles and accessories) of 564 and received 2.321 million visits globally in February 2025.

fitgirl-repacks.site

The video game industry reported *fitgirl-repacks.site* for inclusion in the Watch List for making available infringing download links for PC game titles.

fitgirl-repacks.site had a global SimilarWeb ranking of 2 143, industry ranking (video games consoles and accessories) of 59 and received 23.46 million visits globally in February 2025.

Pirlo TV

Rightholders in ***sports events*** have reported *Pirlo TV* for inclusion in the Watch List as it refers to a significant network of pirate websites. The volume and diversity of pirated content is reportedly enormous and varies according to the sporting events taking place on any given day. It is blocked in Spain by a ruling[90] that allows a dynamic blocking of pirate websites and platforms on a weekly basis.

Pirlotv.fr had a global SimilarWeb ranking of 4 154, industry ranking (soccer) 34 and received 13.15 million visits globally in February 2025.

3.2.4 Peer-to-peer and BitTorrent indexing websites

Peer-to-peer and BitTorrent indexing websites use the peer-to-peer file distribution technology to allow users to share content[91]. The websites act as aggregators of peer-to- peer links, which users can search for and access via the website. When a user clicks on a link, the peer-to-peer technology allows the user to download media files stored on other users' computers across the peer-to-peer network. A user in a peer-to-peer network downloads files from other users' private storage place and makes their own files available for upload to the peer-to-peer network. Users offering a file are known as 'seeders' and they share these files with other users known as 'peers'.

The users need to download a BitTorrent client, the software that will accept a torrent file and begin downloading the data associated with it. Indexing services usually generate income from advertisements and donations from users. BitTorrent indexing sites often register multiple domain names, allegedly in order to prevent their business from being damaged if enforcement authorities seize or block one of their domain names.

[88] https://cuii.info/fileadmin/files/Empfehlung_04-2021_geschwaerzt.pdf
[89] News item: https://www.ouest-france.fr/gaming/nintendo-la-justice-restreint-l-acces-a-des-sites-de-telechargement-de-jeux-video-pirates-7b59560a-9ef7-11ec-a3cc-6629c7a7ad92.
[90] Ruling No. 955/2021 of the Commercial Court No. 6 of Barcelona, 21 December 2021.
[91] EUIPO, Research on Online Business Models Infringing Intellectual Property Rights Phase 1: Establishing an overview of online business models infringing intellectual property rights, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_ex_sum_en.pdf.

As reported by stakeholders from ***the audiovisual and music sectors***, BitTorrent indexing websites remain a major issue as they are still widely used. According to the input from the music industry[92], in the twelve months to April 2023, users illegally downloaded 3.7 billion individual music tracks via Bit Torrent.

The Pirate Bay - ThePirateBay.org, pirateproxy.space, thepiratebays.com

Stakeholders from ***the audiovisual and music industries*** continue reporting *The Pirate Bay* and its proxies for inclusion in this Watch List. Available in 35 languages, *The Pirate Bay* allegedly remains one of the largest BitTorrent websites globally. It facilitates the sharing of all kinds of content (including films, books, music, TV programmes, software and videogames) in its peer-to-peer network. The hosting location of the website is kept hidden. As reported previously, successful legal action concerning this website includes criminal and civil sanctions against its operators as well as its blocking in 22 jurisdictions, such as Argentina[93], Australia[94] ,Austria[95], Belgium[96], Bulgaria[97], Denmark[98], Finland[99], France[100], Iceland[101], India[102], Ireland[103], Italy[104], Malaysia[105], Netherlands[106], Norway[107], Portugal[108], Romania[109], Singapore[110], Spain[111],

[92] See contribution by IFPI, at https://circabc.europa.eu/ui/group/e9d50ad8-e41f-4379-839a-fdfe08f0aa96/library/dba7a3e4-8e6b-4586-b266-bdbeb89b172c?p=1&n=10&sort=modified_DESC.
[93] Juzgado de lo Civil 64, expte. N° 67921/2013, 11 March 2014
[94] Federal Court of Australia, No. NSD 239 and 241 of 2016, 15 December 2016: http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca1503 and Federal Court of Australia, No. NSD 269 of 2017, 18 August 2017: http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca0965
[95] Supreme Court of Austria, No. 4 Ob 121/17y, 24 October 2017: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=df3a2cab-8dd1-4ce4-8795-%209cdfffc0e919&Position=1&Abfrage=Justiz&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=%20&AenderungenSeit=Undefined&SucheNachRechtssatz=False&SucheNachText=True&GZ=4Ob121%2f1%207y&VonDatum=&BisDatum=09.11.2017&Norm=&ImRisSeit=Undefined&ResultPageSize=100&Suchw%20orte=&Dokumentnummer=JJT_20171024_OGH0002_0040OB00121_17Y0000_000
[96] Court of Appeal of Antwerpen, Section 1, No. 3399 Rep. 2011/8314, 26 September 2011: https://nurpa.be/files/20111004_BAF-Belgacom-Telenet-DNS-blocking.pdf
[97] Sofia City Court Bulgaria, Bulgarian Association of Music Producers v. Fiber 1 and Ors., 31 May 2023.
[98] Danish Supreme Court, Telenor v IFPI, No. 159/2009, 27 May 2010: http://www.hoejesteret.dk/hoejesteret/nyheder/Afgorelser/Documents/153-2009.pdf
[99] District Court of Helsinki, Case No. H 11/20937, 26 October 2011.
[100] Court of Appeal of Paris, Case No. 15/02735, 18 October 2016.
[101] District Court of Reykjavik, Case No. E-3784/2015, 17 October 2016: https://www.heradsdomstolar.is/default.aspx?pageid=347c3bb1-8926-11e5-80c6-005056bc6a40&id=31e3ef7d-7b6f-48a7-85b6-a74cb6bfbf95
[102] High Court of Delhi at New Delhi, CS (COMM) 724/2017 & Ors., 10 April 2019: https://spicyip.com/wp-content/uploads/2019/04/UTV-v-1337x-10.04.20191.pdf
[103] High Court of Ireland, Case No. 2008 1601 P ([2009] IECH 411), 24 July 2009.
[104] Supreme Court of Cassation, Judgment no. 49437, 23 December 2009.
[105] Ministry of Domestic Trade Co-operatives and Consumerism (MDTCC), 9 March 2015.
[106] District Court of The Hague, Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v. Ziggo BV, Case No. 365643 –KG ZA 10-573, 19 July 2010: https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBSGR:2010:BN1445&showbutton=true&keyword=brein%20ziggo
[107] Borgating Court of Appeal, Nordic Records Norway AS v Telenor ASA, 9 February 2010.
[108] District Court of Lisbon, No 153/14.0YHLSB, 169605, 4 February 2015.
[109] Tribunalul București, NR. 2229/2018, 5 November 2018.
[110] High Court of the Republic of Singapore, Case No.: HC/OS 95/2018, 26 April 2018.
[111] Central Court of Administrative Litigation Madrid, N66028, 25 March 2015.

Sweden[112] and the United Kingdom[113]. The CJEU has also confirmed that *The Pirate Bay* infringes copyright[114]. However, the service reportedly continues operating through multiple alternative domains hosted in various countries around the world.

ThePirateBay.org had a global SimilarWeb ranking of 1 821, industry ranking (File Sharing and Hosting) of 15 and received 23.31 million visits globally in February 2025.

Rutracker - Rutracker.org

Stakeholders from ***the audiovisual industry*** continue reporting *Rutracker* for inclusion in the Watch List.

Rutracker is a BitTorrent website that has around 2 million active torrents and 13.9 million registered users and is one of the world's most visited pirate websites. The site is hosted in Russia by a Seychelles company. The site is reported to have been subject to blocking orders in several countries, such as Australia[115], Brazil[116], Denmark[117], India[118], Indonesia[119], Italy[120], Malaysia[121], Russia[122] and Singapore[123].

Rutracker.org had a global SimilarWeb ranking of 1 166, industry ranking (file sharing and hosting) of 13 and received 30.45 million visits globally in February 2025.

1337x - 1337x.to

Stakeholders from ***the audiovisual and publishing industries*** continue reporting *1337x* and its proxies for inclusion in the Watch List. The site has several mirror sites/alternate URLs: *1337x.st, x1337x.se, x1337x.eu*.

1337x is a BitTorrent website that allegedly allows users to download films, TV programmes, music, games and apps. The identification of its actual host is not possible, as the site is masked behind a reverse proxy service. Legal action concerning this website includes judgment or

[112] Stockholm District Court, Case Name B 13301-06, and Swedish Patent and Market Court, Case No. PMT 7262-18, 15 October 2018.
[113] High Court of Justice, Chancery Division, Case No. HC11C04518 ([2012] EWHC 268 (Ch)], 20 February 2012.
[114] Judgment of the Court on case C-610/15: https://curia.europa.eu/juris/document/document.jsf?text=&docid=191707&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2184518
[115] Federal Court of Australia, 20 December 2018, Roadshow Films Pty Ltd. and Ors. v. Telstra Corp. Ltd. and Ors., NSD1246/2018.
[116] Criminal District Court Recife (Pernambuco), 7 July 2021 (Operation 404.3).
[117] District Court Fredriksberg, Rights Alliance Denmark v. Banedanmark and Ors., 11 April 2019.
[118] Delhi High Court, 19 September 2019, Warner Bros. Ent. Inc. and Ors. v. RuTracker[.]org and Ors., CS(COMM) 515/2019.
[119] First blocked through administrative order in 2020.
[120] Italian Regulatory Authority for Communications, Decision 33/20/CSP of 13 February 2020, https://www.agcom.it/provvedimenti/delibera-33-20-csp.
[121] First blocked through administrative order in 2023.
[122] News item: https://www.themoscowtimes.com/2015/11/09/moscow-court-orders-torrents-site-rutrackerorg-blocked-for-good-a50678
[123] High Court of the Republic of Singapore, Case No.: HC/OS 95/2018, 26 April 2018.

blocking orders in Australia[124], Austria[125], Belgium[126], India[127], Indonesia[128], Italy[129], Malaysia[130], Netherlands[131], Portugal[132], Singapore[133], Spain[134], and Sweden[135].

1337x.to had a global SimilarWeb ranking of 886, industry ranking (computers electronics and technology) of 33 and received 36.60 million visits globally in February 2025.

Interplanetary Distributed Literature Catalog (IPDL)

IPDL was reported by ***book publishers*** for inclusion in the Watch List. IPDL is reported to be an illegal website that shares and links to the database from other shadow libraries, such as *Library Genesis*, *Sci-Hub*, and *Anna's Archive*, which host and/or direct users to books, articles, media, and other materials available for download illegally.

.

InterPlanetary File System (IPFS)

IPFS was reported by ***book publishers*** for inclusion in the Watch List. It is a decentralized peer-to-peer (P2P) network for distributing, storing and sharing content. Super Pirate and the major pirate networks, including *Library Genesis* (*LibGen*), *Z-Library*, *Anna's Archive* are reported to use public gateways to host and distribute copyrighted materials on IPFS.

3.2.5 Unlicensed download sites

Unlicensed download sites include sites offering direct downloads of the content for free or against the payment of a fee.

Sites selling the content do so at a significantly lower price than the licensed services. The appearance of these sites is sometimes that of legitimate download services, thus confusing users. The prices normally vary depending on the size of the file. These sites often offer new releases as well. As these sites allegedly do not pay royalties, they have presumably lower

[124] https://www.comcourts.gov.au/file/Federal/P/NSD663/2017/3787886/event/29056799/document/1018339
[125] Supreme Court of Austria, No. 4 Ob 121/17y, 24 October 2017: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=df3a2cab-8dd1-4ce4-8795-9cdfffc0e919&Position=1&Abfrage=Justiz&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=&AenderungenSeit=Undefined&SucheNachRechtssatz=False&SucheNachText=True&GZ=4Ob121%2f17y&VonDatum=&BisDatum=09.11.2017&Norm=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=JJT_20171024_OGH0002_0040OB00121_17Y0000_000.
[126] Jugement du Tribunal de commerce francophone de Bruxelles, rép. 004235; A/18/00217, 30 mars 2018.
[127] High Court of Delhi at New Delhi, CS (COMM) 724/2017 & Ors., 10 April 2019: https://spicyip.com/wp-content/uploads/2019/04/UTV-v-1337x-10.04.20191.pdf
[128] First blocked through an administrative order in 2017.
[129]Italian Regulatory Authority for Communications (AGCOM), Decision 110/18/CSP of 8 May 2018: https://www.agcom.it/provvedimenti/delibera-110-18-csp.
[130] First blocked through an administrative order in 2017.
[131] District Court Rotterdam, Stichting Brein v. Delta Fiber Nederland B.V., 24 March 2022.
[132] IGAC, MAPINET v. Artelecom and Ors., 20 October 2015.
[133] High Court of the Republic of Singapore, Case No.: HC/OS 95/2018, 26 April 2018.
[134] Juzgado de lo Mercantil nº 1 de Barcelona, sentencia nº 22/2019.
[135] Patents and Market Court, Aktiebolaget Svensk Filmindustri and Ors. v. Telia Sverige AB and Ors., 24 April 2024.

operation costs, thus likely competing unfairly with legitimate download services and reducing sales of licensed sites.

Sites offering the download of content files for free sometimes base their business model on revenues from advertising. Others operate to provide a free repository of content, mostly publications, often accepting donations from their users.

Sci-hub.io (Sci-hub.tw; sci-hub.cc; sci-hub.ac; sci-hub.bz and others)

Stakeholders from ***the publishing industry*** continue reporting *Sci-hub.tw* and its mirror sites as the most problematic online actors for scientific, technical and medical (STM) and scholarly publishers. As explained in previous editions, *Sci-hub.tw* and its operator are allegedly hosted in Russia. The site reportedly provides unauthorised access to around 80 million journal articles and various academic papers and is said to be hosted in Russia. The site describes itself as 'the first pirate website in the world to provide mass and public access to tens of millions of research papers'. It also explains that it 'provides access to hundreds of thousands research papers every day, effectively bypassing any paywalls and restrictions.' As reported in 2020, legal action concerning this operator includes an injunction issued by United States' courts ordering the domain registries to suspend *Sci-hub.tw's* and its mirror sites' domain names in 2015 and a judgment by the United States' district court in the Southern District of New York[136], which ruled that the site was liable for wilful infringement of copyright. Sci-hub has also been subject to an injunction in France[137] and a court-issued orders were obtained for the blocking of access to Sci-Hub in Denmark[138].

Sci-hub allegedly gains unauthorised access to publishers' journal databases by using compromised user credentials obtained via phishing frauds[139]. Once it gains access to the journal databases, it downloads articles, stores them on its own servers and makes them available to the requesting users, while continuing to cross-post these articles to the *Library Genesis* (see below) and its related sites. The site promotes donations from users as a means to obtain revenue.

Publishers report that *Sci-Hub* changes domain frequently in attempts to obfuscate rights owner enforcement activities. Despite a sequence of legal and website disruptive activities over a number of years including multiple blocking actions around the world, the Sci-Hub network is reported to be still in operation across a number of jurisdictions. It is on the blacklist of manifestly counterfeiting websites of French authority ARCOM[140].

Sci-hub.se had a global Similar Web ranking of 5 231, industry ranking (science and education) of 12, and 10,63 million visits globally in February 2025.

---

[136] Southern New York District Court, 15 civ. 4282 (RWS), 28 October 2015: https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2015cv04282/442951/53/.
[137] https://cdn2.nextinpact.com/medias/jugement-sci-hub-mars-2019.pdf.
[138] Retten I Holbæk Retsbog, Sag BS-25268/2019-HBK, 18 September 2019.
[139] Universities and other institutions have reported instances to the European book publishing industry whereby their students and academic personnel have been subject to phishing frauds. For instance, emails claiming that a student's library access is due to expire and the individual is required to "update" his/her login credentials through a conveniently provided link (that harvests the individual's personal, private information).
[140] https://www.arcom.fr/se-documenter/espace-juridique/decisions/decision-ndeg-2024-408-du-2-mai-2024-portant-inscription-du-service-sci-hub-sur-la-liste-mentionnee-au-i-de-larticle-l-331-25-du-code-de-la-propriete-intellectuelle.

Sci-hub.tw had a global SimilarWeb ranking of 456 620, industry (science and education) ranking of 1797 and 246 850 visits globally in February 2025.

Sci-hub.io had a global SimilarWeb ranking of 9 496 432, industry ranking (science and education) of 21 595 and received 1056 visits globally in February 2025.

Library Genesis - Libgen.onl and mirror sites

Stakeholders from the publishing industry also continue reporting websites related to the so-called *Library Genesis Group* for inclusion in this Watch List. As reported in the previous editions, the *Library Genesis Group* has been active as a website since 2008, where it operated under *libgen.org*. Following legal action, including blocking injunctions or orders issued by the Italian Regulatory Authority for Communications (AGCOM)[141] and by courts in France[142], Greece[143], Russia[144] and the United Kingdom[145], it has shut down and reopened with different names and mirror sites over the years. *Libgen.onl* is hosted in both Russia and the Netherlands. It allegedly operates a repository of pirated publications, including books, scientific, technical and medical journal articles as well as scholarly materials.

Stakeholders from the publishing industry reported that the site now has a main portal under *libgen.onl*, which provides instructions and updates and lists a series of URLs. They reportedly obtain the vast majority of the scientific, technical and medical journal articles via Sci-hub (see above). The site states: '*At Library Genesis, you can choose from more than 2.4 million non-fiction books, 80 million science magazine articles, 2.2 million fiction books, 0.4 million magazine issues, and 2 million comics strips*.'

Other mirror sites associated with the Library Genesis Project include: *bookfi.org, bookzz.org, bookre.org, booksc.org, book4you.org, bookos-z1.org, booksee.org, and b-ok.org*. *Libgen* network is still in operation across a number of domains including *http://libgen.gs/* (indicated as a copy of originals), *http://libgen.rs/, https://www.libgen.is, http://libgen.st/ and https://libgen.lc* (indicated as copy of originals). Sites in the *Library Genesis Group*, as well as proxies are reported to remain subject of a blocking order[146]. The site and some of its mirrors are also subject to blocking orders in the Belgium[147], Denmark[148], France[149], Netherlands[150]. *Bookfi.net* is subject to a blocking order in the UK[151] and in Denmark[152].

---

[141] Italian Regulatory Authority for Communications (AGCOM), Decision n. 179/18/CSP, 25 July 2018: https://www.agcom.it/provvedimenti/delibera-179-18-csp

[142] Tribunal de Grande Instance de Paris, jugement, 7 March 2019: https://cdn2.nextinpact.com/medias/jugement-sci-hub-mars-2019.pdf

[143] https://opi.gr/images/epitropi/edppi_list_v6.pdf.

[144] News item: https://www.chemistryworld.com/news/sci-hub-blocked-in-russia-following-ruling-by-moscow-court/3009838.article

[145] The High Court of Justice, Chancery division, Intellectual Property, HC-2015-001166, 19 May 2015 and The High Court of Justice, Business and Property Courts of England and Wales, Intellectual Property List (ChD), HC-2015-001166, 26 November 2024.

[146] News item: https://blog.magenta.at/2022/08/29/netzsperre/

[147] Decision of the Belgian company court, A/19/03087, 13 November 2019.

[148] Retten I Holbæk Retsbog, Sag BS-25268/2019-HBK, 18 September 2019.

[149] Decision of the Paris Court of First Instance, N° RG 22/09999, N° Portalis 352J-W-B7G-CXXOA, 20 October 2022; Decision of the Paris Court of First Instance, N° RG 20/10567, N° Portalis 352J-W-B7E-CTCI3, 18 December 2020; Decision of the Paris Court of First Instance, N° RG 18/14194, N° Portalis 352J-W-B7C-COMWM, 7 March 2019.

[150] Decision of the Rotterdam District Court, C/10/673460 / KG ZA 24-118, 15 March 2024

[151] The High Court of Justice, Chancery division, Intellectual Property, HC-2015-001166, 19 May 2015.

[152] Retten I Holbæk Retsbog, Sag BS-13084/2018-HBK, 28 May 2018.

Libgen.onl had a global SimilarWeb ranking of 35 181, industry (education) ranking of 1 100 and received 4.028 million visits globally in February 2025.

Libgen.is had a global SimilarWeb ranking of 4 149 industry (science and education) ranking of 10 and received 44,54 million total visits globally in February 2025.

3.2.6 Piracy Apps

As described in Section 3.1, with the increase in the number and users accessing content on mobile hand devices and other connected devices, a whole new ecosystem of piracy apps has emerged where users move from browser-based piracy to app-based piracy using mobile devices and other connected devices[153]. Generally, they are on offer on a website that provides the portal through which the app can be downloaded. These apps are often a subscription-based service, tricking users into believing the legality of the underlying service. Once downloaded and/or registered/subscribed, these apps provide users access to myriad pirate music, movie and television titles. A big number of apps have been reported by ***the audiovisual sector, including sports events organisers,*** as well as music sector.

IPTV Smarters/ WHMCS Smarters

Stakeholders from ***the audiovisual sector*** continue to report *Smarters* for inclusion in the Watch List. It is reported to be an IPTV software solution, which trades under the brand name *WHMCS Smarters* and sells the software, tools, and services that an individual would need to establish and operate his or her own 'off the shelf' illegal IPTV business. *WHMCS Smarters* also provides the IPTV Smarters Pro App, a video player configured for different types of platforms that allows users to watch live television, movies and TV series on demand, and TV catch-up on their devices.

The website *iptvsmarters.com* had a global SimilarWeb ranking of 36 207, industry (web hosting and domain names) ranking of 166 and received and 1.492 million visits globally in February 2025.

EVPAD (ievpad.com)

Stakeholders from ***the audiovisual sector*** continued to report *Evpad* for inclusion in the Watch List as an Android app from China that incorporates P2P technology as well as EVPAD- branded apps to enable access to more than 2 000 movies and TV titles and over 1 000 live international channels. It operates through a network of online and physical resellers around the world, with resellers in over 70 physical locations. The devices are allegedly also sold on popular online marketplaces. It is reported to regularly launch new product lines, including a new brand, 'EVBOX' targeting among others also European customers.

MagisTV, MagisTV.video/magistv-pc.info

[153] EUIPO, Discussion paper, *APPS & APP STORES - Challenges and good practices to prevent the use of apps and app stores for IP infringement activities*, Alicante, 2024, https://data.europa.eu/doi/10.2814/788692.

Stakeholders from ***the audiovisual and sports sectors*** reported *MagisTV video* as the most widespread illegal IPTV platform in Latin America.

Magistv-pc.com had a global SimilarWeb ranking of 13 854, industry ranking of 543 and received 19.59 million visits globally in February 2025.

Magistvvideo.com had a global SimilarWeb ranking of 259 664, industry (search engines) ranking of 2 388 and received 968,149 million visits globally in February 2025.

3.2.7 Hosting providers, including dedicated server providers

Pirate sites often depend on hosting providers, including dedicated server providers (DSPs), that provide the necessary infrastructure for them to operate (for instance easy access or fast download).

The term 'hosting providers' can cover a broad range of hosting services which can for example be distinguished by the type of IT resources made available to clients, and the degree to which these providers manage the services necessary to make a content available on the Internet, with the exception of managing the content itself.

IT resource needs may vary depending, among others, on the type of content distributed. In some cases, the computing power of a physical server can be shared between several clients and their websites, and the hosting provider manages the server. In other cases, like for example streaming of audiovisual content to a large public, physical servers may need to be fully dedicated to this task for performance reasons.

DSPs make such physical servers available to clients, including network connectivity. Clients can either manage their dedicated servers completely on their own, or choose a DSP which offers server management services (such management services can also be offered by third-party providers). Some hosting providers have policies against infringers and regularly take action to prevent pirate sites from using their services for copyright infringements. However, others do not follow due diligence to prevent websites from using their services for illegal activities. Likewise, some hosting providers do not cooperate with copyright holders in removing or blocking access to pirate content. A significant number of hosting providers and DSPs has been reported by stakeholders. A number of the services mentioned below are reported by stakeholders to openly advertise that they will not respond to take down requests from content owners. The possibility of assessing the popularity of these services is limited and therefore no figures on ranking and visits are provided.

DDoS-Guard.net

DDoS-Guard.net (also reported to operate as *Cognitive Cloud L.P.*) is again reported by ***the audiovisual sector*** for inclusion in the Watch List as a 'bulletproof' hosting provider for pirate sites. Many piracy sites including *s.to* and *bs.to* are reported to be relying on Ddos- Guard's services for hosting. Rightholders report the service as not responding to takedown notices.

Private Layer

Stakeholders from different sectors, in particular from ***the audiovisual and sports industries***, continue reporting *Private Layer* for inclusion in this Watch List.

Private Layer allegedly provides anonymity to the owners and operators of the websites that use its services. It reportedly hosts infringing sites and refuses to respond to outreach notices from rightholders.

Virtual Systems, V-Sys

Stakeholders from ***the audiovisual and sports industries*** reported *Virtual Systems* for inclusion in this Watch List. *Virtual Systems* is a hosting provider for infringing sites providing content from VOD streaming websites, IPTV services and sports live streaming websites.

Squitter, ABC Consultancy, Peenq, ESTOXY, BestDC, SERDECHS (also sometimes referred to as *ABC Consultancy*) is a DSP, which is reported as a fast-growing hosting provider for infringing sites. As other hosting providers take action removing infringing content, *Squitter* is reported to be the replacement destination of choice for many pirates. The service changes name regularly, making it more difficult to track.

Besides the above services, a number of DSPs have been reported by ***the audiovisual sector***, notably by the sports events organisers, as not responding to take down requests and not taking any action to avoid infringements of copyright. While many legitimate companies do comply with take down requests, the internet piracy landscape has evolved in such a way that pirates have tended to cluster around hosting providers which do not comply in a timely manner. They are often established in 'offshore' jurisdictions, or mask their identities and locations, in such a way as to avoid legal liability to content infringements happening on their infrastructure. In fact, some of these hosting providers advertise themselves as non-compliant with takedown requests.

Amarutu Technology Ltd ('Amarutu', also known as Koddos)

Amarutu is reported to be a DSP, which claims to have office locations in Hong Kong (China) and Seychelles. It is reported by rightholders to consistently ignore their takedown notices. Some stakeholders report, however, the diminished level of infringements and no longer report the DSP as a priority.

AS-Istqservers / Istqserverses ('Istq')

Istq is reported to be a Jordanian DSP that operates multiple ASNs[154] that is still responsible for many infringing live streams and fails to take any meaningful action upon receipt of takedown notices.

HostPalace Web Solution PVT LTD ('Host Palace')

Host Palace is reported by stakeholders to be an Indian DSP, which continues to be responsible for high volumes of infringing live streams and not taking any action to cease copyright infringements.

[154] Autonomous System Numbers (ASNs) are allocated by Internet Assigned Numbers Authority (IANA) and are used by various routing protocols, see: https://www.iana.org/assignments/as-numbers/as-numbers.xhtml

3.2.8 Unlicensed IPTV services

As explained in the trends section above, unlicensed IPTV services offer without authorisation access via streaming to hundreds or even thousands of TV channels illegally.

Stakeholders from ***the audiovisual and broadcasting industries*** have reported the websites below as examples of illegal IPTC services for inclusion in the Watch List. They allegedly sell subscriptions for unlicensed IPTV services. Data on the popularity of these websites is difficult to gather. The SimilarWeb ranking of use of the websites is less relevant than in other services mentioned in this Watch List, as users may only visit the site to purchase a subscription.

King365tv.com / Theking365tv.pro, Theking365tv.site

King365tv has again been reported by the stakeholders from ***the audiovisual sector*** for inclusion in the Watch List. It reportedly operates from Algeria and gives access to over 2 200 international channels and an extensive VOD library.

VolkaIPTV.com/ Redirects to volkalive.ru

VolkaIPTV.com is also reported again by stakeholders from ***the audiovisual sector*** for inclusion in the Watch List. It reportedly operates from Algeria or Morocco and offers a reseller programme and customer plans of various IPTV services that provide access to about 7 500 international TV channels, as well as 17 000 films and 1 000 TV series, at low monthly subscription fees. Its estimated audience is 60 000 users.

GenIPTV

Reported by stakeholders in ***the audiovisual sector*** for inclusion in the Watch List, Gen IPTV is claimed to be one of the largest IPTV providers in the world, with over 10 000 international channels and 52 000 VOD titles.

Dark IPTV

Reported by stakeholders in ***the audiovisual sector*** for inclusion in the Watch List, *Dark IPTV* has been gaining prominence in recent months. Main categories of pirated content distributed or available on the website (e.g. films, music, books, live content). The main domain is blocked in Spain[155] through a ruling that allows a dynamic blocking of pirate websites and platforms on a weekly basis.

3.2.9 Piracy supporting services

As described in the previous edition of the Watch List, these services provide a suite of off-the-shelf services that make it easy for would-be pirates to create, operate, and monetise a fully functioning pirate operation. They are reported to include, for example, website templates that facilitate setup of streaming websites, databases providing access to tens of thousands of infringing movies and TV series, in exchange for payment of a fee or a cut of the advertising

[155] Ruling No. 955/2021 of the Commercial Court No. 6 of Barcelona dated 21 December 2021.

revenue, dashboards that allow an illegal IPTV operator to oversee the infrastructure of their service, hosting providers that provide a safe haven for pirates, video hosting services that obscure links to infringing content and decentralised streaming software that acts as a third party tool between a streaming site and a cyberlocker or video host, allowing for quicker upload of content with a large variety of cyberlockers and video hosting services.

2embed.ru; 2embed, or 2embed[.]cc / 2embed[.]skin

2embed.ru has again been reported by stakeholders in ***the audiovisual sector*** for inclusion in the Watch List as a pirate content management system (CMS) library. The site's CMS is reported to crawl various websites and search engines to find movie and TV show streaming links which are then stored in their database and served through their application programming interface (API) service. It offers a large library of movies via streaming, direct link, or embedding. *2embed* provides its service for free and remunerates itself by inserting ads. Rightholders report that despite their and anti-piracy trade associations' successful enforcement action in July 2023 to shut down *2embed[.]to*, which was run from Vietnam, the site is operating again using different domains such as *2embed.cc* and *2embed.skin*. *2embed* is an example of a Platform as a Service (PaaS) provider that significantly contributes to the global trade in pirated content by offering services that make it easy for other bad actors to create, operate, and monetize fully functioning piracy operations.

2embed.cc had a global SimilarWeb ranking of 358 804and received 113 871 visits in February 2025.

Vidsrc[.]to

Vidsrc has been reported by rightholders in ***the audiovisual sector*** for inclusion in the Watch List. It is reported to be a popular video library used by *Fmovies* and over 500 dedicated piracy sites. The service provides an enforcement resistant library of content to piracy sites. Its operators are believed to be based in Vietnam. In August 2024, *Vidsrc[.]to* was taken down, resulting in hundreds of sites depending on the video library going offline as well.

Vidsrc.me had a global SimilarWeb ranking of 70 164, industry rank (TV movies and streaming) of 2 403 and received 3.141 million visits in February 2025.

Njal[.]la – 1337 Services (St Kitts and Nevis)

Njalla, located at *njal[.]*, has been reported by rightholders in ***the audiovisual sector*** for inclusion in the Watch List. *Njalla* is reported to be prominent among pirate services, with customers such as *FlixTor[.]se*, and *ygg[.]re, Collaps.org* . This off-the-shelf piracy facilitation service makes it easy for would-be pirates to create and monetise a fully functioning pirate service.

Njal.la had a global SimilarWeb ranking of 350 824, industry rank (web hosting and domain names) 1 460 and received 270 988 visits in February 2025.

GDrivePlayer

GDriveplayer.to has been reported by rightholders in ***the audiovisual sector*** for inclusion in the Watch List. It is reported to offer various simple-to-use APIs for operators of pirate streaming services to source lists of links to infringing video content hosted on Google Drive, Google Photo, Youtube and Facebook.

GDriveplayer.to had a global SimilarWeb ranking of 417 048, industry rank (social networks and online communication) 3 507 and received 430 934 visits in February 2025.

4. E-COMMERCE PLATFORMS AND SOCIAL MEDIA PLATFORMS

4.1 E-commerce platforms

E-commerce platforms offer a convenient, efficient, and secure way to buy and sell products or services online. According to the Eurobarometer[156] carried out in 2024, 77% of respondents in the EU bought or ordered products or services online in the 12 months preceding the survey. At the same time, these platforms can be misused by merchants who seek to deceive online shoppers and distribute counterfeit goods. Consumers find it difficult to distinguish between genuine and fake goods, especially online. Consumers may therefore be led to believe that the product they buy is genuine, only to discover a counterfeit delivered to their homes. In a recent study by EUIPO[157], 15% of Europeans said they have unintentionally bought counterfeit in the last 12 months, as a result of being misled. Moreover, 39% said they have found themselves in a situation where they have wondered whether the product they bought was counterfeit or not.

The sale of counterfeit goods over the internet presents a threat considering that: (i) consumers are at a growing risk of buying sub-standard and possibly dangerous goods, (ii) the brand image and economic interests of EU companies are damaged through the sale of counterfeit versions of their products, and (iii) the efforts of e-commerce platforms to be regarded as safe places to purchase legitimate products are undermined.

The Commission has been increasing efforts to tackle the threat of illegal content or products through different measures, including, the *Digital Services Act* (DSA)[158], adopted on 19 October 2022, a *Recommendation on combatting online piracy of sports and other live events*[159], adopted on 4 May 2023, and a *Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights*[160], adopted on 18 March 2024.

Various obligations imposed by the DSA are instrumental in improving the fight against illegal content, including counterfeiting and piracy. This is, for instance, the case with the designation

[156] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals .
[157] EUIPO, *European Citizens and Intellectual Property: Perception, Awareness, and Behaviour – 2023*, Alicante, 2023, https://data.europa.eu/doi/10.2814/87818.
[158] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, p.1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.
[159] Commission Recommendation (EU) 2023/1018 of 4 May 2023 on combating online piracy of sports and other live events C/2023/2853, OJ L 136, 24.5.2023, p. 83, ELI: http://data.europa.eu/eli/reco/2023/1018/oj.
[160] Commission Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights, C/2024/1739 final, 19.3. 2024, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:C(2024)1739.

of points of contact and legal representatives, the requirements on terms and conditions, the transparency reporting obligations, the notice and action mechanisms, the complaint and redress mechanism, the trusted flagger mechanism, measures and protection against misuse. Additional measures apply to online marketplaces, which must ensure the traceability of traders (known as know-your-business-customer (KYBC) obligations), the compliance by design and the right to information. Moreover, very large online platforms and very large online search engines must comply with the most stringent rules of the DSA, such as assessing, analysing and mitigating a wide array of systemic risks, including the dissemination of illegal content through their services.

The 2018 *Recommendation on measures to effectively tackle illegal content online*[161] identified best practices, which online platforms are encouraged to follow in order to reduce the availability of illegal content, including counterfeit offers on e-commerce websites. It aimed in particular at clearer notice and action procedures, more effective tools and proactive measures to detect and remove counterfeit listings and other illegal content, more transparency on online platforms and closer cooperation with trusted flaggers, rightholders and enforcement authorities.

The 2023 *Recommendation on live events piracy*[162] prompts action from hosting service providers to address illegal streaming of live events, encourages the use of dynamic injunctions to block illegal streaming of live events, recommends increasing the availability and affordability of commercial offers and calls on Member States to raise users' awareness on legal offers of live events and on the issue of piracy.

The 2024 *Recommendation on combatting counterfeiting*[163] focuses on strengthening cooperation through single contact points for IP enforcement and extending the use of existing tools such as the IP Enforcement Portal. The Recommendation also highlights good practices that can be employed by intermediary service providers, such as transport and logistic service providers, payment service providers, social media providers and domain names providers in the fight against IP infringements. It also aims at enhancing enforcement by encouraging, for example, signatories of the *Memorandum of Understanding on the sale of counterfeit goods on the internet* to use the 'trusted flagger status' under the DSA, and at ensuring future-proof IP protection by adapting legal procedures to counter new counterfeiting practices like mirror website with dynamic injections.

Most recently, the Commission published the Communication on the E-commerce[164], *A comprehensive EU toolbox for safe and sustainable e-commerce*, which refers to the developments in the area of e-commerce including some risks related to the increased flow into the EU of low-value and/or illegal products, including counterfeits, via e-commerce platforms. Counterfeit products not only harm the economic interests of rightholders but they may also present health and safety risks for consumers. The Communication sets out a comprehensive strategy how to deal with these risks.

In the course of the public consultation for the preparation of the Watch List, stakeholders acknowledged that e-commerce platforms do not infringe IPR directly or base their business

[161] Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, C/2018/1177, OJ L 63, 6.3.2018, p. 50, ELI: http://data.europa.eu/eli/reco/2018/334/oj.
[162] See footnote 159
[163]See footnote 160
[164] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive EU toolbox for safe and sustainable e-commerce, COM(2025) 37 final, 5.2.2025, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0037.

models on activities that infringe IPR. In several cases, stakeholders also reported positive experiences and developments. However, overall rightholders continued to report a high number of e-commerce platforms from a variety of countries which they consider did not take sufficiently efficient measures to tackle offers of IPR-infringing goods made by sellers who use these platforms.

The section on e-commerce platforms of this Watch List describes some developments with reported e-commerce platforms. This includes both the progress made in some areas and the ongoing concerns regarding e-commerce platforms that are still considered to lack sufficient measures or require significant improvements.

When assessing the measures taken by the e-commerce platforms to avoid counterfeiting, the following aspects were considered: the estimated amount of counterfeit goods offered on their platforms, the effectiveness of the measures to detect and remove counterfeit offers and/or the level of cooperation with rightholders and enforcement authorities. Other factors reported such as the lack of clarity of the platforms' terms of service regarding prohibiting their use to sell or otherwise trade in counterfeit goods and services, the absence of effective vetting of the sellers who are trading on the platforms, or the absence of repeat infringer policies were also considered.

As in previous years, a number of stakeholders nominated several major global or regional platforms, such as platforms operated by Alibaba (*Aliexpress.com*, *Tmall.com*, *Taobao.com*, *1688.com*), Amazon *(Amazon.com*), Meta (*Facebook*), Mercado Libre, which, according to them, still have many counterfeit goods on offer. At the same time, it is noted that these platforms have taken a number of measures in line with the industry best practices. Several of these e-commerce platforms have reported on a range of measures to prevent and filter offers for counterfeits and have been cooperating with law enforcement authorities and rightholders. Some of them are signatories of the *Memorandum of Understanding on the sale of counterfeit goods via the internet*[165], which is an industry-led cooperation managed by the European Commission that provides a platform for members to discuss practical issues such as new trends, challenges and technological tools in the fight against counterfeiting, individually and collectively. Taking into consideration the engagement of these operators in the fight against counterfeiting, these platforms can overall be considered as adhering to a good industry standard, while they still need to continue making efforts and cooperate further with rightholders and law enforcement authorities.

Updates by e-commerce platforms that required further monitoring

Some e-commerce platforms, previously listed as having made progress but requiring further monitoring, provided updates on the measures taken and fulfilment of the commitments made to enhance efforts against piracy and counterfeiting since the last edition of the Watch List.

In this context ***Shopee,*** which is one of the biggest business-to-consumers online e-commerce platforms in Southeast Asia but also present in Brazil and Mexico, was again reported by stakeholders for allegedly selling a high volume of counterfeit goods, especially in Latin American countries. It was also reported as lacking progress in dealing with repeat offenders or

[165] *Memorandum of Understanding on the sale of counterfeit goods on the internet* (the territorial scope of the MoU is limited to the activities of the signatories within the EU/EEA), https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-sale-counterfeit-goods-internet_en.

high-risk infringers. Some specific issues, such as limits to daily reports and a too lenient policy on sellers of counterfeits were also reported. *Shopee* has from its side reported on a number of improvements, such as the introduction in 2024 of a dedicated Test Purchase Program for its Southeast Asian markets to identify and test products for counterfeit goods, focusing on those that could pose health and safety risks. Reportedly, sellers of counterfeit products face immediate removal of the listings and potential permanent closure of their shops. *Shopee* reported that in the past year, their Brand IP Portal saw a significant increase of 289% in registered users and 235% in registered IP certificates. According to *Shopee*, they review and process notifications by rightholders within three days on average, with approximately 94% of reported listings successfully removed upon the first notification. Furthermore, *Shopee* indicated that in May 2024 they introduced a feature allowing users to report impersonating sellers at the shop level. They have also increased the maximum number of reportable listings per case from 200 to 1 000 in July 2024. Regarding proactive detection measures, they reported on improvements in their in-house trademark infringement detection data science model. On repeat offenders, Shopee reported on the penalty points based system leading to a progressive loss of privileges for sellers and stated to have strengthened the KYBC policy across the markets in 2024.

Some stakeholders also continued reporting ***DHgate*** which is the largest business-to-business e-commerce platform in China, for allegedly selling high volume of counterfeit goods. *DHgate* has from its side reported to have implemented some proactive measures to block counterfeit items. In 2023, *DHgate* published a report[166] which includes an overview of their proactive measures, of their seller verification system and of their cooperation with rightholders and law enforcement authorities. For example, regarding proactive measures, they report improvements in their machine recognition with an extension from simple image and text recognition to 'image + video' review, better data performance in the keyword recognition system, brand logo model, and imitating image model, with some figures. They also report on increased external cooperation with rightholders, industry associations, compliant agencies, and regulatory authorities. *DHgate* is to publish a new IP Protection report in 2025.

These updates reported by *Shopee* and *DHgate* show further improvements since the last edition of the Watch List in 2022, but the efficiency of the measures taken and potential additional efforts need to be monitored also in the future.

The last edition of the Watch List included ***Tokopedia***, one of the most popular business-to-consumers and business-to-business e-commerce platforms in Indonesia. *Tokopedia* was reported as a platform that was deemed not have taken sufficient measures. Stakeholders reported *Tokopedia* also for this edition of the Watch List due to their alleged reluctance to engage with rightholders, highly ineffective measures and the fact that, despite the implementation of notice and takedowns, the volume of infringing products has not declined. Rightholders also reported some worsening of the situation after Bytedance's acquisition of a majority stake in *Tokopedia* in early 2024. Allegedly, some new programmes, such as proactive enforcement and online to offline enforcement were put on hold indefinitely. In its submission, *Tokopedia* has from its side reported on their proactive measures, which combine the use of different tools such as Detection Engine and image recognition tools. They reported that 80% of infringements on their service were removed through the proactive measures. They also reported on their IP Protection Portal, which facilitates the submission of notice and take down requests by rightholders, an average resolution time of IP claims of 48 hours and a success rate of 98% as well as their three-strike system for repeated infringers,additional measures for

[166] https://brand.dhgate.com/intellectualproperty/2023_IP_PROTECTION_REPORT_0401.pdf.

pharmaceutical products and cooperation with rightholders, public authorities and law enforcement. Due to the differences in the input provided by stakeholders and the platform, some further monitoring is needed to assess the effectiveness of the measures taken by Tokopedia.

E-commerce platforms where no progress has been reported

Regarding e-commerce platforms, which are deemed not to have taken enough measures and have not made submissions, stakeholders continue to report a number of platforms in Russia with high numbers of counterfeits but which either are reluctant to take any measures or are not responsive to requests for removals of counterfeits. These include ***Avito.ru***, ***Tiu.ru, Youla.ru.*** Stakeholders also continue to report ***Deal.by*** (Belarus) and ***Satu.kz*** (Kazakhstan). All these marketplaces were nominated again because of a cumbersome takedown procedure, which includes overly burdensome administrative requirements, the overly long processing time to handle complaints, the lack of proactive measures and repeat infringers policy, as well as lack of cooperation with rightholders.

4.2 Social media platforms

Social media platforms enable end-users to communicate online and share content on different privacy levels (public, semi-public, private), primarily for private but also for commercial purposes. Stakeholders generally acknowledge that the social media platforms that they reported did not have as the main or one of the main purposes to infringe copyright. Nor do they seem to base their business models on activities that infringe copyright. However, stakeholders report that groups in social media are increasingly used to share copyright-protected content without authorisation. Due to the popularity of these groups, tens of thousands of users have access to this illegal content. Some social media users also use their individual accounts to offer or promote illegal services, including IPTV services.

The contributions received for this Watch List outline again the increasing use of social media in sharing of links to infringing services and facilitating access to counterfeit goods across different communication channels.

The alleged misuse primarily consists of directing unsuspecting users attracted by official brand images or guided by other users or content providers, including so-called influencers (via links or otherwise) to third-party websites or cloud storage services where content can be streamed or downloaded, or counterfeits are offered for sale. This trend has also been outlined in the EUIPO discussion paper[167] about the evolving nature of social media services in infringing IP rights. According to this paper, infringers are able to reach a broad range of consumers by means of sponsored advertisements and direct them to external websites offering counterfeit products or IPR- infringing content. Advertisements of well-known brands on websites and mobile apps lead consumers to believe they acquire legally published content or original goods or services, thereby damaging the brands' reputations as well. Furthermore, information on where and how to access IPR infringing content and goods may be shared amongst users in invite-only groups or otherwise, followed-up by private messages. This may also circumvent IP protection measures and poses challenges to tracing infringing activities. This difficulty, also due to the sheer volume of traffic, is apparent from the EUIPO report on *Monitoring and analysing social*

[167] EUIPO, Social Media - Discussion Paper - New and existing trends in using social media for IP infringements activities and good practices to address them, Alicante, 2021, https://data.europa.eu/doi/10.2814/272629.

media in relation to IP infringement from 2021[168] demonstrating that social media platforms are tools for recurrent IPR infringements for digital content and physical products[169]. In addition, integrative and constantly changing functions of social media platforms, coupled with their global use across borders, make it difficult to navigate for IP rightholders and enforcement authorities.

Stakeholders from different sectors continued to report concerns with regard to ***Telegram***, for features that allow users to share unauthorised content with a significant number of users through a group or via channels for broadcasting to unlimited audiences[170]. More specifically, rightholders reported that the channels allow to transmit content to an unlimited number of subscribers, including to push infringing content to subscribers for download and/or streaming. According to rightholders, channels typically include a search functionality which allows subscribers to easily locate content and/or include a browsable menu of all available content. It is also reported that bots, i.e. third-party applications that operate within *Telegram*, can be used as specialised search engines to locate specific content available on the service. Finally, rightholders reported that content can be shared between individuals within groups which can have up to 200 000 members. Despite some improvements in compliance rates for the removal of infringing links and channels, rightholders indicated that *Telegram's* response to takedown notices varies from almost immediate to no response in spite of multiple re-notifications. For example, it is reported that *Telegram* processes requests to remove non-linear contents illegally hosted on the platform, while it rarely considers notifications of illegal live streaming of events. *Telegram* allegedly also ignores requests to remove groups/accounts selling IPTV subscriptions. Stakeholders outlined concerns with inconsistent enforcement of *Telegram's* repeat infringer policy. According to the information provided by rightholders, they have brought successful enforcement actions against *Telegram* in India[171], Israel[172], Italy[173] and Portugal[174] requiring *Telegram* to provide operator information and block access to infringing content.

[168] EUIPO, Monitoring and analysing social media in relation to IPR infringement, Alicante, 2021, https://data.europa.eu/doi/10.2814/235275.

[169] It may be exemplified by conversations related to different product categories for which social media may be misemployed as search engines for content and products, such as counterfeit medicines (pharma related conversations suspected of referring to counterfeit medicines peaking twice depending on the lockdown measures back in 2020).

[170] See description of Telegram's services at Telegram FAQ: https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here.

[171] In January 2022, in proceedings for an interim order, the Delhi High Court granted interim relief to rights holder Doctutorials Edutech Pvt Ltd ordering Telegram to take down unauthorised copyright-protected material posted on channels. Telegram was also ordered to provide details of offending parties that it has available. In the High Court of Delhi at New Delhi + CS(COMM) 60/2022 & I.A. No. 1338/2022 (O-39 R-1 & 2) Doctutorials Edutech Private Limited v Telegram FZ-LLC & ORS.

[172] CA 24999-02-20 ZIRA (Copyright on the Internet) Ltd. et al. v. Telegram Messenger Llp et al., Decision of the Central-Lod District Court of Israel, 04 February 2021.

[173] For example, the Italian Federation of Newspaper Publishers (FIEG) filed an application with AGCOM in relation to Telegram channels that were illegally distributing unauthorised copies of newspaper publications. Following the complaint, an Italian prosecutor issued an emergency order in April 2020 requiring Telegram to shut down the infringing channels, failing which, AGCOM would require internet service providers to block access to the entire Telegram service in Italy. Telegram subsequently shut down the relevant channels.

[174] In November 2021, in proceedings for injunctive relief, the IP Court of Lisbon ordered Telegram to block access to 17 channels, devoted to online piracy, with over ten million members combined in an action brought by Visapress (Gestão de Conteúdos dos Médiato) and GEDIPE (Associação para a Gestão de Direitos de Autor, Produtores e Editores) acting on behalf of publishers and the film industry respectively, Reference: 461343 Precautionary Procedure (CPC2013) No. 520/20.0YHLSB, Applicant: Visapress - Gestão de Conteúdos dos Media, Crl and Others, Defendant: Telegram FZ-LLC, Date: 15 November 2021.

Telegram reported from its side on the content monitoring systems and policies and procedures that they apply to detect and remove potentially illicit content and to ban or restrict accounts (users and bots),groups and channels that promote or encourage the sharing of illegal content. *Telegram* referred to continuous reviewing of content on their platform, which includes measures to prevent automated content distribution, proactive review of public content both via technical solutions, including AI, and qualified moderators. *Telegram* underlined that users only encounter content they explicitly choose to engage with. *Telegram* also indicated that as they restrict all forms of bulk activity across their platform, including the mass sending and forwarding of messages, promotional content, and media in private chats, secret chats, groups, and channels, as well as the importing of contacts and the use of search functionality, the systemic dissemination of IP infringing material is restricted by design. Regarding notice and takedown requests by rightholders, *Telegram* reported on the means for rightholders to submit the takedown requests and indicated that complaints are typically handled without delay, but processing times can vary depending on the clarity and completeness of the specific claim while on average not exceeding 24 hours. Regarding repeat infringer policy, *Telegram* explained that recurrent unauthorized sharing of copyrighted material may result in account suspensions, while more serious or systematic infringements can lead to permanent bans and a proactive review and takedown of any related communities. In some cases, the administrators' accounts may also be permanently blocked to prevent the creation of new communities intended to facilitate further infringement. Regarding measures against live streaming, *Telegram* indicated that live streamed content is not indexed in search and can only be accessed via a direct link or by specifically searching for and joining a specific channel or group. According to *Telegram*, live streams are never inserted into users' message flows or between community posts, which means that the exposure to live streams remains entirely user-initiated. If malicious actors attempt to bypass these limitations *Telegram* reported that their anti-spam system automatically detects and blocks such behaviour and accounts involved in this type of activity are swiftly restricted. *Telegram* mentioned that it is currently exploring several new features that will allow for expedited addressing of live streamed content with the assistance of several trusted organizations. Finally, *Telegram* described their cooperation with different rightholders and external stakeholders, including authorities.

Overall, stakeholders reported many social media platforms, both global and regional or local ones[175], with different degrees of concerns mainly related to their cooperation with rightholders and notice and take-down actions. As most of the services take some measures against IP infringements, which may however be limited due to the nature of the services, and the difficulties of assessing the effectiveness of measures taken by social media platform, this edition of the Watch List does not list new social media platforms, which, however, does not mean that there are no concerns with these services – they need to be monitored for further efforts to avoid illegal activities. Social media platforms offering their services in the EU have to comply with the obligations under the DSA.

Among social media platforms reported, ***VK .com (V Kontakte),*** which was listed in the previous Watch List remains problematic. *VK.com* is a social network based in Russia but available in many languages, including English. It is the leading social network in Russia and Russian speaking territories. Rightholders report that *VK.com* users can have unauthorised access to films and TV shows, including via embedded video players. This occurs in groups where users can share, upload and download content. A search function makes it relatively easy for users to find the infringing content. Other stakeholders report a significant number of counterfeits in their service. Stakeholders also report that whilst *VK* used to be responsive to takedown notices,

[175] Such as X (former Twitter), The Little Red Book (China) etc.

they now ignore most of them and continue to be a significant infringement hub. According to rightholders, since 2022 *VK's* compliance with takedown notices has fluctuated, with inconsistent results at times dropping to 30% and below by 2024. The site has been blocked subject to criminal blocking orders in Italy. No new information was provided by *VK.com* for the purposes of this edition of the Watch List.

VK.com had a global SimilarWeb ranking of 29 and in Russia 4, industry rank (social networks and online communication) of 9, and 3.137 billion visits in February 2025.

5. ONLINE PHARMACIES AND SERVICE PROVIDERS FACILITATING THE SALES OF MEDICINES

The counterfeiting of pharmaceutical products, driven by transnational organised crime networks, represents a growing threat within the EU. This highly profitable form of international trafficking incentivises the involvement of more criminal groups to enter the business. While counterfeit pharmaceuticals pose significant risks to public health and safety, affecting not only individuals but also national healthcare systems, pharmaceutical crime leads to substantial financial losses for the legitimate pharmaceutical sector, damaging brand reputation and undermining investment in research and development.

The need to address counterfeiting of pharmaceutical products in the EU is supported by the data provided in the study *Why Do Countries Import Fakes? OECD/EUIPO 2023*[176], in which six EU Member States (Germany, Belgium, Italy, France, the Netherlands and Spain) figure in the list of top 15 importers of counterfeit pharmaceutical by volume worldwide.

The report *EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2023, November 2024*[177], by the Commission and the EUIPO, indicated India (68.69%) and China (6.85%) as main countries of provenance for medical products (medicines and other products (condoms)).

According to the *Joint EUIPO-Europol report Uncovering the ecosystem of Intellectual Property crime - A focus on enablers and impact from November 2024*[178], criminals involved in pharmaceutical fraud target a broad spectrum of products, including anticonvulsants, antiepileptic drugs, synthetic opioids, anti-cancer treatments, erectile dysfunction and antidiabetic medications, pseudoephedrine, doping substances (e.g. hormone and metabolic regulators) and others.

As detailed in the report *Illicit trade in fakes under COVID-19* (OECD/EUIPO)[179], the COVID pandemic created new opportunities for criminal networks engaged in the illicit trade of counterfeit goods. Despite the initial decline in counterfeit products, the rise in fake COVID-related items, such as personal protective equipment, test kits, and medicines, ensued. As the demand for these items grew, counterfeit operations expanded to include a broader range of

[176] OECD/EUIPO, *Why do countries import fakes? Linkages and correlations with main socio-economic indicators*, OECD Publishing, Paris, 2023, https://doi.org/10.1787/8a4a4508-en.
[177] European Commission: Directorate-General for Taxation and European Union Intellectual Property Office, *EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2023*, Alicante, 2024, https://taxation-customs.ec.europa.eu/document/download/67bd3b33-c597-47d5-aae9-c7336f60d6fe.
[178] Europol/EUIPO, *Uncovering the Ecosystem of Intellectual Property Crime: A focus on enablers and impact*, Alicante, 2024, https://data.europa.eu/doi/10.2814/1947113.
[179] OECD/EUIPO, *Illicit trade in fakes under the COVID-19*, OECD Publishing, Paris, 2024, https://doi.org/10.1787/0c475a23-en.

products, capitalising on the surge in online shopping which remains a lasting consequence of the COVID pandemic.

A common method of operation involves the diversion of medicines from the legal supply chain through illicit acquisition - such as falsified or stolen prescriptions or unauthorized sales - driven by market demand, the value of the medicines, and challenges in the legal supply system. The trade in illicit pharmaceuticals primarily occurs on the surface web, where targeted advertisements on social media or instant messaging apps lead to temporary websites that often mimic well-known e-commerce platforms. However, there is a growing trend of using dark web marketplaces for the sale of counterfeit pharmaceuticals, as these platforms provide greater anonymity, making it more difficult to identify and dismantle illegal operations. Criminal actors also utilize instant messaging apps and dark web marketplaces to target customers outside the EU.

The illicit supply caters to specific demand. Criminals involved in the sale of hormonal substances often infiltrate the fitness industry, particularly gyms, where these products are in high demand. Social commerce, facilitated by social media influencers who promote both legitimate brands and counterfeit products - often knowingly - through their self-proclaimed 'dietary and nutrition' channels, is becoming a major marketing tool for illicit hormonal substances.

The abuse of prescription and over-the-counter medications, along with other health products for recreational purposes, psychoactive effects, weight loss, performance enhancement, and cosmetic use, is expected to continue growing. This increasing demand will inevitably provide ongoing opportunities for organised crime groups.

Stakeholders have identified and reported significant concerns across both social media platforms and marketplace-commerce platforms, where numerous prescription pharmaceuticals are offered without the requirement of a valid prescription. Furthermore, they reported that non-compliant pharmaceutical product listings are widespread on websites, with a particularly troubling rise in illicit offers for weight loss medications. This trend appears to be driven by heightened demand for weight loss products, increased public awareness, and ongoing shortages, creating opportunities for counterfeit and fraudulent activities.

The global trafficking of counterfeit medicine is combated by a number of regional and global initiatives. The fourth edition of Operation SHIELD[180] was conducted between April and October 2023, coordinated by the EUROPOL, whereby 30 countries across 3 continents joined forces in the fight against trafficking of counterfeit medicines and illicit doping substances. Operation SHIELD found that illegal vendors continue to advertise doping substances on social media platforms, mostly targeting non-professional athletes and members of restricted or private sport groups. Along with performance-enhancing products, medicines for erectile dysfunction are offered via dubious channels online and remain among the most seized counterfeits by law enforcement. Operation SHIELD resulted in charges against 1 284 individuals and total seizures worth above EUR 64 million, dismantling of four underground labs, and shutting down of 92 websites.

Furthermore, Operation Pangea XVI[181], which ran in October 2023 and was coordinated by the INTERPOL has led to 72 arrests worldwide, the seizure counterfeit pharmaceuticals worth more

[180] News item: https://www.europol.europa.eu/media-press/newsroom/news/fake-medicines-worth-eur-64-million-eu-markets

[181] News item: https://www.interpol.int/en/News-and-Events/News/2023/Global-illicit-medicines-targeted-by-INTERPOL-operation

than USD 7 million (EUR 6,755,698.39), 325 new investigations and the closure of more than 1 300 criminal websites. Erectile dysfunction medications accounted for 22% of seizures during the operation and being the most seized medicine globally, followed by psychotherapeutic agents such as antidepressants, anti-anxiety medicines and stimulants which accounted for 19%, and by sex hormones and gastrointestinal medicines which accounted for 12% each. These actions highlight the ongoing necessity for a coordinated, global response to the threat posed by illicit medicines and transnational organised crime networks.

6. PHYSICAL MARKETPLACES

Stakeholders from various industry sectors have reported a significant number of physical marketplaces worldwide. The majority of the goods involved are consumer items, including clothing, fashion accessories, eyewear, perfumes, bags and suitcases, watches, electrical appliances, stationary, and toys, predominantly sold in shopping malls or open market (bazaar-type) settings. For consumers frequenting these markets it may not be immediately apparent that these goods are counterfeits, nor are they likely to be aware of the potential health and safety risks associated with such products.

The selection of the marketplaces for the following listing is based on a set of criteria designed to identify those most likely to cause harm for IP rightholders from the EU. Marketplaces reported by multiple stakeholders supported by verifiable information have a higher likelihood of appearing on the list. In addition to factors such as the estimated size and volume of sales, the level of overt IPR infringements and the proportion of displayed IPR infringing goods were also considered. Furthermore, actions taken to address the availability of IPR infringing goods are reflected in the listing below as the Watch List aims to encourage further actions by the market operators and local enforcement authorities.

The listing of physical markets is intended to be illustrative and is presented alphabetically by the country in which they are located. In some regions, counterfeit goods are commonly sold across borders in physical markets. Therefore, the inclusion of physical markets in one country does not mean that significant IPR infringements do not occur in markets of the neighbouring countries. For example, in Latin America, in addition to the markets in the countries listed below, stakeholders have reported on numerous marketplaces in Bolivia, Paraguay, Uruguay and Peru, although limited details have been provided about the location and the type of goods sold. Additionally, some stakeholders may no longer report certain marketplaces despite their possible continuous operation.

For marketplaces comprehensively described in the previous editions of the Watch List, this edition provides less detailed information. However, this does not diminish the actual importance of these markets. The Commission will continue to use stakeholders' information provided on marketplaces not listed, especially in cooperation with EU's trading partners, through IP dialogues, working groups, and technical cooperation activities.

Argentina

La Salada with its sub-markets (*Punta Mogotes*, *Hurkupiña and Ocean*) in Buenos Aires and *La Salada de Mendoza* in Santa Rosa (Mendoza Province), continue to be reported by several stakeholders as among the biggest (wholesale) marketplaces of counterfeits in Argentina and beyond. Another example of the reported markets of counterfeits is the *Once Neighbourhood* in Buenos Aires.

Counterfeits are often imported from other countries but also produced locally in unauthorized factories. Despite multiple attempts by the Argentinian authorities to shut down or regulate these markets, they continue to flourish.

In 2024, Argentinian authorities took several actions to combat the trade in counterfeits. In particular, the customs authorities seized more than 6 tons of clothing and shoes in the port of Buenos Aires and more than 600 million pesos (548 000 EUR) in counterfeit merchandise in the airport of Ezeiza. Furthermore, in the same year, tax authorities detected illegal merchandise valued at more than 200 million pesos (180 000 EUR) in different stores selling men's and women's clothing in the center of the city of Mendoza.

Bosnia and Herzegovina

Stakeholders referred to the *Arizona* market, a vast informal market in Brčko with approximately 2000 stores and 4500 employees close to the border with Croatia with alleged cross-border supply chains and wholesale activities for a wide range of counterfeit goods. According to stakeholders, parts of the goods are delivered unbranded to the market, where the respective trademarks are then affixed to the goods before they are being offered for sale. Due to the complex system of competences between different enforcement institutions in BiH (market inspections, police and prosecutor offices, from Federation of BiH, Republika Srpska and Brčko District) raids are purportedly difficult to initiate.

Brazil

Several stakeholders continue to report the markets in the *Rua 25 de Março* area of São Paulo as the epicentre of wholesale and retail activities for counterfeits in Brazil. Enforcement operations mentioned in the previous Watch List are reported again and refer to some success. Also reported by stakeholders is the 'Shopping 25 Brás' mall which contains nearly 200 shops selling counterfeit electronics, clothes and toys. It attracted attention in late October 2024 when a fire engulfed much of it so is currently temporarily closed.

Nova Serrana in Minas Gerais State is again reported as a major production site for counterfeit sport shoes and household goods, sold across Brazil and other Latin American countries. Enforcement actions against manufacturers and distributors have been conducted upon requests by IP rightholders. In October 2024, following a complaint from a rightsholder, police seized thousands of pairs of counterfeit shoes heading from Nova Serrana to the Brás area of São Paulo. Days later, police in Nova Serrana intercepted another shipment of shoes, imitating various international sport brands, whose destination was Foz do Iguaçu at the border with Paraguay and Argentina. The seizures were part of a joint campaign with an industry association, which estimates that counterfeit footwear is distributed mostly in small shops or door-to-door in person, rather than online.

Stakeholders also report marketplaces in other cities such as the *Feirão des Malhas* in Rio de Janeiro or *Feire de importados* in Brasilia.

The Brazilian authorities have made significant efforts to address the problem of counterfeiting. The most recent enforcement actions in 2024 were the *Operation Fake Brand* in which more than 20,000 counterfeit items bearing 24 different trademarks were seized, including clothes, perfumes, glasses, and watches; *Operation Blackbeard*, which brought together over 100 public authorities to seize counterfeit goods across Brazil; *Operation Tsuru* in which the Liberdade

neighbourhood in São Paulo was raided and BRL 1 million (EUR 160 000) in counterfeit handbags, shoes, backpacks, and other accessories was seized; *Operation Bad Toys* in São Paulo targeted a warehouse selling counterfeit toys online; *Operation This Is Not a Toy* in which 3 tons of toys from physical shops in São Paulo were seized; *Operation Pinocchio* in the state of Mato Grosso targeting physical shops and distribution networks of toys priced at 10 to 15% of the originals.

In September 2024, Brazilian customs intercepted eight false-bottom trucks crossing a bridge from Paraguay, with a cargo of counterfeit tyres, auto parts, and pesticides, in addition to conventional and electronic cigarettes, with a total estimated value of BRL 10 million (EUR 1.6 million). In the same month they also seized 4 tons of counterfeit electronics, mobile phones and accessories worth more than BRL 2 million (EUR 320 000) at seven locations in Rio Grande do Sul.

China

Stakeholders continue to report a high number of markets across China, often entirely dedicated to the sale of a wide range of counterfeits. Law enforcement authorities regularly conduct raids but even civil and criminal convictions of direct infringers do not appear to affect the operation of the markets in the longer term, with offers for counterfeits becoming less blatant at best. For some markets, stakeholders complain about a lack of inspection and enforcement activities in the first place.

Markets listed in the 2020 Watch List and 2022 Watch List have been reported again, in particular the *Asia Pacific Xingyang Fashion and Gifts Plaza* in Shanghai, the *Anfu* market in Putian City (according to stakeholders with some sellers moving their business to sell counterfeits online), the *Mule Town* in Guangxi Province and the *Silk Market* in Beijing.

Other markets reported by stakeholders include: the *Zhanxi Apparel Mall* engaging in the sale of medium to low-end clothing and accessories, the *Xinbaijia Apparel Online Trade Market*, mainly selling sportswear and football uniforms, the *Guangzhou Baiyun World Leather Trading Center*, all in Guangzhou, Guangdong Province; the *Luohu Commercial City* in Luohu District, Shenzhen City, Guangdong Province; the *Yiwu Int'l Trade Mart* in Yiwu City, Zhejiang Province, selling clothes, accessories, perfumes and cosmetics; the *Dajingkou Shoes & Clothing Market*. Qingyang Town, Jinjiang City, Fujian Province; the *Xingwang International Clothing Market* in Hongkou District, Shanghai; the *Shenyang Wu Ai Market* in Shenhe District, Shenyang.

Stakeholders also reported Anxin County, Baoding City, Hebei Province as becoming the largest source of counterfeit footwear in Northern China, with several factories presumed to be manufacturing counterfeits despite several successful criminal actions conducted previously, although only very limited enforcement actions have occurred in Anxin in 2024. Another area reported by stakeholders is Chenhai City, Shantou, which is listed for its toys and gifts industry.

Colombia

The *San Andresitos* markets encompassing numerous shopping centres in different areas of Bogota (San Andresito San Jose, San Andresito de la 38, San Andresito del Norte) with thousands of stalls selling high volumes of counterfeit goods for a variety of consumer goods

such as footwear, apparel, food, detergents, cosmetics, fashion products, bags, watches, jewellery etc., have been reported again by several stakeholders.

According to the input received, regular enforcement actions were carried out with the support of the local police and there are several pending criminal and administrative proceedings against the owners and/or workers of the stores and warehouses involved in selling counterfeit goods. Many rightholders report having conducted enforcement actions with the help of Colombian authorities, to seize goods from the stalls and to raise awareness about potential dangers of counterfeits for consumers.

India

Stakeholders continue to report *Karol Bagh* and adjacent markets of *Gaffar and Tank Road* for the inclusion in the Watch List. Located in Delhi, these markets are among the largest in India, with a reputation for allegedly selling counterfeit goods. They are said to offer a wide range of counterfeit products, including sports equipment, footwear, clothing, electronics, luxury items, watches, and cosmetics. Although successful civil and criminal enforcement actions have been performed, including decrees obtained from courts, permanent injunction and monetary recoveries, these efforts have not proven sufficiently effective in curbing the issue.

Stakeholders have also reported significant quantities of counterfeit goods at various other marketplaces across India, including *Crawford market, Heera Panna market and Chawls of Mumbai* in Mumbai, the *Rabindra Sarani, Burra Bazar, New Market* and *Khidderpore* in Kolkota.

Indonesia

Mangga Dua Market and *Tanah Abang Market*, both located in Jakarta with hundreds of shops, as described in the 2018 and 2020 Watch Lists, were reported again by several stakeholders. Conducted raids, if any, remain ineffective to combat the rampant sale of counterfeit goods on retail and wholesale basis.

In addition, as in the 2020 and 2022 Watch List, marketplaces in other parts of Indonesia allegedly offer counterfeits in high volumes as well, particularly in Banten and on Bali, catering for tourists.

Malaysia

The *Petaling Street Market, Plaza TAR* and the *Berjaya Times Square* shopping complex in Kuala Lumpur are yet again reported by stakeholders as places with high volumes of counterfeits offered for sale, despite raids initiated by rightholders in some of those markets.

Local authorities are reportedly unresponsive to the complaints by rightholders, with only a few enforcement actions taking place, attributed to an alleged lack of manpower within the enforcement agencies. Additionally, stakeholders have reported substantial quantities of counterfeit goods at various other markets across Malaysia, including the *SG Wang*, the *Kenanga Shopping Mall* and *GM Plaza* in Kuala Lumpur, the *Batu Ferringhi Night Market* in Penang, as well as the *KSL City Mall* in Johor Bahru.

Mexico

The *El Tepito* open air market in downtown Mexico City and the *San Juan de Dios* market in Guadalajara, both of which have been previously identified by stakeholders as some of the largest indoor markets in Latin America and described in more detail in the previous Watch List, have been reported once again for their alleged ongoing involvement in the sale of counterfeit goods. As highlighted in the previous Watch List, these markets continue to be significant hubs for both retail and wholesale distribution of high volume counterfeit goods. Despite repeated reporting, there appears to be no meaningful progress in addressing the issue, and efforts to curtail the widespread sale of counterfeit goods remain largely ineffective.

Morocco

Souk Korea and *Derb Soltan Fida* market in Casablanca as well as *Djamaa El Fna and Mohamed V* in Marrakesh, remain central open markets with vast offers for counterfeit goods. These include perfumes, eyewear, footwear, fashion items, sporting goods (primarily sports shoes, football, and basketball jerseys), and handbags. However, as reported, the issue persists across a broader scope of marketplaces beyond the above-mentioned locations.

A significant portion of counterfeit goods is reported to be manufactured in Morocco. However, no verified sources could confirm that thus raising doubts about the accuracy of such claims, especially as some market sellers assert that counterfeits produced in Morocco have a higher perceived value than those from Asia.

Several enforcement measures have been taken by Moroccan authorities to combat the proliferation of counterfeit goods. Customs authorities occasionally conduct raids in shops and warehouses targeting counterfeit goods. In 2023, customs authorities reported the seizure of over 1.8 million counterfeit goods, with a total estimated value of 21 million dirhams. Stakeholders report that public authorities take insufficient actions, information on imminent raids is leaked and any possible raids face resistance. Endeavours to enforce IP rights in civil proceedings are allegedly futile as well.

Philippines

Stakeholders continue to report *Baclaran* and *Divisiora* markets in Manila for offering a wide range of counterfeit goods on wholesale and retail basis, in particular footwear and apparel, with some stalls allegedly also running online shops offering counterfeit goods. According to stakeholders, no police actions are taken. Shops in the *Greenhills Shopping Mall* and *Cartimar* shopping malls and in particular the stalls located in their vicinity are reported to sell higher quality counterfeit goods.

Reportedly, regular raids are conducted by the National Bureau of Investigation and Intellectual Property Rights Division of the Bureau of Customs and although they have had an impact in the past, they are allegedly no longer effective as there are too many infringers and the economic harm remains high.

Russia

The *Sadovod* shopping complex in Moscow, with supposedly more than 100 000 customers per day visiting thousands of stores, was listed by several stakeholders for its widespread offers of counterfeit goods, in particular clothes and shoes, on retail and wholesale basis. The evident

sales of counterfeits have been subject to media coverage but public authorities are reportedly reluctant to take any action despite repeated complaints from rightholders in the past. Some raid actions have been conducted, but there has been little to no progress.

Apart from other markets, stakeholders referred in particular to *Yuzhni Dvor* and *Dubrovka* markets for huge amounts of sales of counterfeit consumer items and for a lack of interventions by public authorities.

Serbia

The *Buvljak open market* in Subotica, close to the Hungarian border, was again reported by stakeholders. This market is one of the biggest in Serbia with almost 2.000 stalls selling a variety of counterfeits, predominately clothing and footwear, originating mostly from China and Türkiye but also with some supplies from local production in Novi Pazar which was mentioned by stakeholders in particular for the production of denim clothing. The market in Novi Pazar was also referred to by stakeholders.

With regard to enforcement, according to the media reports, there are general attempts of different inspections to close down certain shops and stalls which were allegedly pushed back by sellers with limited impact so far and no apparent further actions taken by public authorities. The authorities reported that in the period 2023-2024, 814,887 pieces of clothing, sports equipment and various fashion accessories have been confiscated in the area of Novi Pazar and Subotica, for which the authorities had indications that they were intended for sale, among other things, at the location of the *Buvljak open market* in Subotica.

Thailand

Stakeholders continue to report the *MBK Centre, Platinum Market and Patpong Night Market* in Bangkok, as the main markets where counterfeit products, such as clothing, apparel, footwear, and handbags, are offered for sale.

The *MBK Centre* features hundreds of shops and stalls visited by tourists, many of which are dedicated to offering almost exclusively counterfeit products. According to the information provided, many shops are not just minor retailers sourcing from local wholesaler but developed enterprises with supply chains for counterfeit goods reaching across borders as far as Vietnam and China. Public authorities show considerable efforts to organize awareness raising campaigns but also, more importantly, to conduct ex officio actions and cooperate closely with rightholders. However, despite frequent raids and official warnings, most sellers continue to offer counterfeit products. Stakeholders assert that legal actions against the operator of the *MBK Centre* cannot be initiated, which reduces the chances of a permanent closure of all shops concerned. Stakeholders also report that enforcement is difficult as there is always leakage of information before the operation.

Similar issues are noted for the *Patpong Night Market* , which is another tourist spot where high volumes of counterfeits are offered for sale. Stakeholders report that while the police gives verbal warning to sellers, they however resume the illicit trade after the police completes the patrol and leaves the market. With regard to shops in the *Platimum Market*, which continue to offer counterfeits as well, rightholders positively note a decrease thereof after action from local law enforcement authorities.

Other markets in cities close to the boarders with Cambodia and Myanmar were mentioned by stakeholders as well.

Türkiye

Stakeholders continue to report The *Grand Bazaar* in Istanbul, which is one of the largest and oldest covered markets in the world, with 61 covered streets and over 4 000 shops which attract between 250 000 and 400 000 visitors daily. It is a major tourist attraction and a place where high quantities of counterfeit good are offered for sale. Stakeholders reported that there is no change despite a number of conducted raids and criminal prosecutions.

Stakeholders reported *Ak Çarşı* wholesale mall as the second biggest marketplace for counterfeit goods in the country, mainly for apparel and footwear. It is claimed that public authorities take no proactive measures, and the responsible operators remain unresponsive to pursuits from rightholders to tackle counterfeiting which has been persistent ant for years. Stakeholders also report that although upon initiative of rightholders several criminal enforcement actions against the market have been undertaken, this has not had any substantive impact on reducing the counterfeits available on this market.

The *Bedesten Çarşısı* market in Izmir, selling allegedly more than 200 000 pairs of counterfeit shoes per year, was reported by various stakeholders. According to the information provided, there has been no activity to remove, limit or discourage the availability of counterfeits in this market for many years.

United Arab Emirates

Stakeholders continue to report the *China Mall* in Ajman, as one of the biggest wholesale and retail distribution centres and transit hubs in the Middle East, where high quantities of counterfeit goods are offered for sale. According to the information provided by stakeholders it is the second largest wholesale distribution centre of Chinese merchandise, with an operating area of 100,000㎡. Despite a number of raids conducted by Ajman authorities inside the mall, this has resulted only in reduced visibility of counterfeits at offer as traders engage in more clandestine sales to trusted groups of resellers.

The *Dragon Mart* in Dubai, advertised as the world's largest Chinese mall and trading hub for Chinese products outside mainland China, was reported again. Stakeholders claim that the raids conducted by the Department of Economic Development agents and the police are not eradicating the sale of counterfeits due to relatively low fines and the limited seizures of counterfeits, which are mostly stored elsewhere.

Several stakeholders referred to the *Karama* shopping complex in Dubai, which despite raids conducted by the Department of Economic Development carries on the sale of counterfeits such as leather goods, shoes or watches.

As reported by stakeholders, trade in counterfeit products remains rampant in the *Jebel Ali Free Zone* in Dubai. Stakeholders emphasize that, despite the Memorandum of Understanding between the Dubai Department for Economic Development and the Dubai Police, allowing it to take actions in this area, sales of counterfeit products have not declined. Other bazars and informal markets, such as Deira (Naif), Satwa, and Gold Souk in Dubai, Bengali Garments Market in Ajman, and Islamic Souk in Sharjah, were reported as well.

Viet Nam

Saigon Square Plaza in Ho Chi Minh City continues to be reported by stakeholders as operating despite regular and repeated raids taking place by law enforcement authorities. Allegedly, fines are low and thus have little deterrent effect. The same applies to *Ben Thanh Market* in Ho Chi Minh City in which reportedly 40% of stores sell counterfeits mainly apparel and accessories such as watches and bags. The *Dong Xuan market* in Hanoi, also formerly featuring in the Watch List, has been reported again, as the wholesale market and the most important marketplace in Hanoi where multiple categories of counterfeit goods are offered for sale.

P. Lương Văn Can Market, *Ninh Hiep Market* and *Chợ Trời Market* in Hanoi, *Móng Cái Market* in Mong Cai City at the border with China, as well as *An Dong Market*, *Bình Tây Market*, *Kim Biên Market*, *Dan Sinh Market*, and *Đ. Trường Chinh* in Ho Chi Minh City, were equally reported by stakeholders for the high amount of counterfeit goods.

ANNEX I
Methodology Used for the Preparation of the Watch List

Sources

The Commission services conducted a public consultation between 4 June and 15 August 2024.[1] Its results form the basis of this Watch List. 52 respondents contributed to the public consultation. The majority of them were brand owners, copyright holders, associations and federations representing rightholders and associations fighting against IP infringements. Other respondents were individuals, law firms and chambers of commerce. A number of online service providers, such as e-commerce platforms and social media platforms, providers of internet infrastructure services or associations of providers of technology products and services also contributed to the public consultation. Information regarding the respondents and their contributions were published on 6 September 2024.[2] Interested stakeholders were invited to submit their observations on the contributions until 18 October 2024 and the observations received were also published.[3]

The Commission services verified to the extent possible the factual statements contained in the contributions to the public consultation against impartial and reliable sources as indicated in this section.

In addition to the support provided by Europol and EUIPO, a number of other sources played a role in the selection process and in defining and describing the marketplaces and service providers mentioned in this Watch List.

Information from the Commission services

- Information received from EU Delegations and Offices;

- Information on IP policy received from Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs and from Directorate-General for Communication Networks, Content and Technology;

- Information received from the Directorate-General for Taxation and Customs Union on customs enforcement of intellectual property rights by EU Member States and information on detentions of IPR infringing goods in the internal market, reported by enforcement authorities of 25 EU Member States through the IP Enforcement Portal (IPEP)[4] ;

- Information gathered via IP Key China[5].

EUIPO reports and studies

---

[1] https://policy.trade.ec.europa.eu/consultations/public-consultation-counterfeit-and-piracy-watch-list-1_en. For further details on the public consultation, see Annex II.

[2] https://circabc.europa.eu/ui/group/e9d50ad8-e41f-4379-839a-fdfe08f0aa96/library/dba7a3e4-8e6b-4586-b266-bdbeb89b172c?p=1&n=10&sort=modified_DESC.

[3] https://circabc.europa.eu/ui/group/e9d50ad8-e41f-4379-839a-fdfe08f0aa96/library/2d7f5d0c-d547-43f1-8a17-c3c77d566a27?p=1.

[4] European Commission: Directorate-General for Taxation and European Union Intellectual Property Office, *EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2023*, Alicante, 2024, https://taxation-customs.ec.europa.eu/document/download/67bd3b33-c597-47d5-aae9-c7336f60d6fe.

- Joint studies by OECD and EUIPO on the economic impact of counterfeiting and piracy and trade in fakes[6] and on the harm to consumers[7];

- Sectoral Studies[8];

- Study on state of online piracy and copyright infringement[9];

- Joint studies by Europol and EUIPO on the ecosystem of IP crime[10]

- EUIPO Discussion papers on search engines[11] , live event piracy[12], and apps and app stores[13].

Other relevant sources

- SimilarWeb[14] popularity ranks;

- Google Transparency Report[15].

Selection of services and marketplaces mentioned in the Watch List

The selection of the service providers and marketplaces in the Watch List aims to provide significant examples of different types of online service providers and physical markets that play, directly or indirectly, a major role in the counterfeiting or piracy of EU IPR- protected goods. The service providers and marketplaces listed in the Watch List were selected between

---

[6] OECD/EUIPO, *Global trade in Fakes. A worrying threat.*, OECD Publishing, Paris, 2021, https://doi.org/10.1787/74c81154-en and OECD/EUIPO, *Why do countries import fakes? Linkages and correlations with main socio-economic indicators*, OECD Publishing, Paris, 2023, https://doi.org/10.1787/8a4a4508-en.

[7] OECD/EUIPO, *Dangerous Fakes: Trade in counterfeit goods that pose health, safety and environmental risks*, OECD Publishing, Paris, 2022, https://doi.org/10.1787/117e352b-en and OECD/EUIPO, *Illicit trade in fakes under the COVID-19*, OECD Publishing, Paris, 2024, https://doi.org/10.1787/0c475a23-en.

[8] EUIPO, *Economic impact of counterfeiting in the clothing, cosmetics, and toy sectors in the EU*, Alicante, 2024, https://data.europa.eu/doi/10.2814/053613.

[9] EUIPO, *Online copyright infringement in the European Union – films, music, publications, software and TV (2017-2023)*, Alicante, 2023, https://data.europa.eu/doi/10.2814/966644.

[10] Europol/EUIPO, *Uncovering the Ecosystem of Intellectual Property Crime: A focus on enablers and impact*, Alicante, 2024, https://data.europa.eu/doi/10.2814/1947113.

[11] EUIPO, Discussion paper, *Search Engines – Challenges and good practices to limit search traffic towards intellectual property infringing content and services*, Alicante, 2023, https://data.europa.eu/doi/10.2814/3359064.

[12] EUIPO, Discussion paper, *Live event piracy - Challenges and good practices from online intermediaries to prevent the use of their services for live event piracy*, Alicante 2023, https://data.europa.eu/doi/10.2814/060481.

[13] EUIPO, Discussion paper, *APPS & APP STORES - Challenges and good practices to prevent the use of apps and app stores for IP infringement activities*, Alicante, 2024, https://data.europa.eu/doi/10.2814/788692.

[14] The EUIPO's *Study on Digital Advertising on Suspected Infringing Websites* describes that "SimilarWeb uses big data technology to estimate websites' unique visitors from desktops and the origin of those visits. SimilarWeb provides information on: (1) global rank, rank of site in top country, and category rank (i.e. Rank 15 in the category of File Sharing), as well as the up or down trend in popularity; (2) total visits each month for the past 6 months; (3) traffic sources (35% direct, 33% referrals, 14% search, 7% social); (4) top 5 referring sites and top 5 destination sites; (5) leading organic keywords that users searched that led them to the site; (6) percentage of social networks sending traffic to the site; (7) top ad networks and leading publishers referring advertising traffic to the website; (8) audience interests including a short list of websites frequently visited by the website's users; (9) similar sites and (10) related mobile apps".

[15] Google makes available online at https://transparencyreport.google.com/ a report that indicates the volume of infringement takedown requests sent by parties to Google for search takedowns in relation to websites that may infringe copyright. The copyright related websites listed in this Watch List were cross-checked with the Google Transparency Report for specific organisations to identify websites with the highest number of infringing link notices sent to Google by key IP rightholders and other IP content protection associations.

November 2024 and March 2025. Consequently, the information included in the report reflects the situation during this period.

All selected service providers and marketplaces are located outside the EU to the knowledge of the Commission services. Online marketplaces and service providers are considered to be located outside the EU for the purposes of the Watch List if their operator or owner is known or assumed to be resident outside the EU, irrespective of the residence of the domain name registry, the registrar, the residence of the hosting provider or the targeted country. As regards physical marketplaces, the market is considered located outside the EU if it is physically hosted in the territory of a third country irrespective of the citizenship or residence of its landlord.

Most stakeholders, namely rightholders, that contributed to the public consultation launched by the Commission indicated the service providers and marketplaces that, in their view, should be included in the Watch List (see Annex II for further details). Most of the selected service providers were reported in various contributions, often by stakeholders representing a wide array of sectors.

Other stakeholders such as e-commerce platforms, social media platforms, providers of internet infrastructure services or associations of providers of technology products and services also provided their input in the public consultation, including on measures they take to reduce the availability of counterfeit offers and piracy on their platforms.

Some contributions included detailed explanations of the acts performed by the allegedly infringing service providers or service providers' failings as regards the measures taken to fight illegal content or goods on their services. This is sometimes confirmed by decisions of the national courts of the EU Member States and of third countries declaring the liability of, or blocking access to, the service providers.

Some contributions included a qualitative assessment of the harm caused to the EU industries by certain marketplaces and service providers and included information on their global or regional popularity and high volume of sales of counterfeit or pirated content. In order to identify websites that are popular globally or regionally, SimilarWeb web popularity ranking[16] and Google's Transparency Reports[17] for copyright-related websites were used. Some of the selected marketplaces or service providers are mostly visited from the EU whereas others are visited only from third countries but harm EU rightholders and trade with these countries.

With regard to the measures taken by e-commerce platforms and social media platforms, different elements were considered based on the best practices and industry standards, such as the need for a clear notification procedure, transparent policy for the removal or disabling access to the content, regular activity reports, the use of automated means for the detection of illegal content, cooperation with rightholders and enforcement authorities.

In recent years, further obligations and recommendations have been adopted to strengthen the enforcement of IP rights in the EU. These include the DSA[18], which provides for harmonised rules for a safe, predictable, and trusted online environment and imposes specific obligations on certain specific categories of providers of intermediary services, including online platforms

[16] https://www.similarweb.com/
[17] https://transparencyreport.google.com/copyright/overview?hl=en
[18] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, p.1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

allowing consumers to conclude distance contracts with traders[19]. The Commission has also adopted two Recommendations: the *Recommendation on combating online piracy of sports and other live events*[20], adopted in 2023, and the *Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights*[21], adopted in 2024.

The 'Watch List' does not contain assessments of whether the services mentioned comply with the obligations set in the DSA or follow the different Commission Recommendations in the area of IP enforcement, which are monitored under the relevant instruments.

[19] For the sake of this Watch List the terms 'online service providers' and 'e-commerce platforms' are maintained while it is to be noted that in the DSA, these services are referred to as online intermediary services and online marketplaces.
[20] C (2023) 2853 final, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:C(2023)2853.
[21] Commission Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights, C/2024/1739 final, 19.3. 2024, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:C(2024)1739.

ANNEX II
Overview of the Results of the Public Consultation

Like in previous years, creative industries covering a wide array of sectors, such as music, audiovisual, publishing, TV broadcasting or software, submitted most of the public consultation contributions on piracy. The contributions from broadcasters or organisers of broadcast sport events remained numerous, showing a continuous and an increasing concern about the proliferation of operators engaged in the provision of unlicensed IPTV services and some new trends.

A wide range of services were reported again, with an increase in some new forms of piracy. Among the most reported services were linking websites, cyberlockers, unlicensed IPTV operators, peer-to-peer networks and BitTorrent indexing websites and stream-ripping services. Some new services and trends were reported which are described in Section 3.

Brand owners (electronics, fashion, footwear, luxury, sporting goods, toys, etc.), brand associations and federations, chambers of commerce, associations fighting against counterfeiting reported mostly physical marketplaces and e-commerce platforms. More than 90 e-commerce platforms or social media platforms were reported for the online distribution of allegedly counterfeit goods. Respondents to the public consultation continued to report concerns about some actors in the online ecosystem which could help to better address the proliferation of pirated content, such as providers of ad networks and social media platforms, as well as Content Delivery Networks[1] (CDNs). What these actors can be expected to take as measures continues to be debated while some new rules under the DSA may be applicable and developing case law may continue bringing further clarifications.

In this context, *Cloudflare*, has been reported again as in previous years. While it is recognized that the services of Cloudflare are not aimed at disseminating infringing content, rightholders indicate that Cloudflare's services can be easily exploited by pirate operators due to the anonymity they can have. At the same time rightholders also reported some measures and cooperation undertaken by Cloudflare with rightholders, such as the 'trusted flagger' system. Among their concerns, rightholders mentioned allegedly poor repeat infringer policy and lack of a meaningful know-your-customer policy of Cloudflare. Rightholders therefore continue calling on Cloudflare to improve further its cooperation with them given its role as a key player in the online environment. Cloudflare from its side reported on their approach to complaints of copyright infringements, which varies depending on the services being used. When Cloudflare provides hosting services, they reported to conduct notice and takedown in response to copyright complaints. Cloudflare also reported that most often they acted as a reverse proxy and CDN service, with no ability to remove content, even though the Cloudflare Internet Protocol addresses may appear in WHOIS and DNS records for websites using their services and, as such, Cloudflare could be erroneously characterised by stakeholders as being the hosting provider. Cloudflare indicated that it provided a mechanism[2] for rightsholders to report perceived

[1] A Content Delivery Network is a geographically distributed network of proxy servers and their data centres that replicates a website's content on each of the servers to allow the downloading of the content from the place that is closest to the user. Content delivery networks (CDNs) increase content delivery speed and capacity and provide security against threats such as hacking or viruses. CDN reverse proxy services protect websites' IP addresses in order to prevent cyberattack. This affects the information provided by the WhoIs Database (an online protocol that is widely used for querying databases that store registered data on the users of a domain name, the IP address, the name of the registrar, starting date and expiration date of the domain name, etc.). For websites using CDNs, WhoIs lists the IP address of the server within the CDN (front host) through which the content is routed and not the server actually hosting the content (back host).

[2] www.cloudflare.com/trust-hub/abuse-approach/ and www.cloudflare.com/trust-hub/reporting-abuse/

infringements on websites using Cloudflare's services. When a valid complaint is filed, Cloudflare forwards the complaint to the site owner and hosting provider for appropriate action. Cloudflare also reported on its Trusted Reporter system that provides additional information to large rightsholder organisations and law enforcement agencies under certain conditions that are necessary for cybersecurity purposes. Finally, Cloudflare reported to have developed an API that enables rightholders to automate their submissions to Cloudflare's reporting form and indicated that they had automated mechanisms to limit their free services from being used to stream content online and violate their terms of service. Cloudflare also collaborates with law enforcement authorities in cases involving large-scale piracy or other serious intellectual property crimes in line with legal standards to protect both the rightholders and the rights of their customers.

Respondents to the public consultation continued to express concerns about the role of certain social media platforms in the distribution of counterfeit goods online. A number of online services were also reported by stakeholders in the context of ad networks supporting illegal activities. Some specific domain name registries have also been reported by rightholders, as not taking sufficient action against pirate websites (.to, .ru, .tv, .bz, .io).

Some e-commerce platforms and social media platforms, as well as other online service providers provided detailed information on the measures they take to reduce the availability of counterfeit offers and piracy on their platforms. Some of e-commerce platforms rely partly on the key performance indicators introduced by the *Memorandum of Understanding on the sale of counterfeit goods via the internet*[3], which is a voluntary agreement facilitated by the European Commission to prevent offers of counterfeit goods from appearing in online marketplaces offering their services in the Member States.

With regard to illicit online pharmacy networks, stakeholders reported that the practices described in the previous Watch List continue, notably the use of domain privacy and proxy services for domain registrations, the use of subdomain to conceal infringing content and the registrations of hundreds of websites funnelling the traffic. Significantly fewer networks and registrars than before were reported in the public consultation for this Watch List, with scarce substantiation of the claimed facts. For this edition, the Commission services therefore refrain from mentioning specific networks.

In some countries, medicines are available via social media platforms or in unregulated open markets, for instance, alongside other day-to-day consumer items. Counterfeit medicines affect the global population but there is a noticeable prevalence of counterfeits including lifesaving medicines, such as antibacterial or antimalarial medicines, in the African region.

Besides specific services and marketplaces, stakeholders reported a number of trends and also some new practices and service providers, which are described in Section 3 of the Watch List.

[3] *Memorandum of Understanding on the sale of counterfeit goods on the internet* (the territorial scope of the MoU is limited to the activities of the signatories within the EU/EEA), https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-sale-counterfeit-goods-internet_en.