The legal framework for video-sharing platforms

IRIS *Plus*

A publication
of the European Audiovisual Observatory

European Audiovisual Observatory

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS *Plus* 2018-1
The legal framework for video-sharing platforms
European Audiovisual Observatory, Strasbourg, 2018
ISSN 2079-1062
ISBN 978-92-871-8608-9 (print edition)

Director of publication – Susanne Nikoltchev, Executive Director
Editorial supervision – Maja Cappello, Head of Department for Legal Information
Editorial team – Francisco Javier Cabrera Blázquez, Sophie Valais
European Audiovisual Observatory

Authors (in alphabetical order)
Francisco Javier Cabrera Blázquez, Maja Cappello, Gilles Fontaine, Ismail Rabie, Sophie Valais
European Audiovisual Observatory

Translation
Michael Finn, Marco Polo Sarl, Stefan Pooth, Ulrike Welsch

Proofreading
Philippe Chesnel, Johanna Fell, Jackie McLelland

Editorial assistant – Sabine Bouajaja
Marketing – Nathalie Fundone, nathalie.fundone@coe.int
Press and Public Relations – Alison Hindhaugh, alison.hindhaugh@coe.int
European Audiovisual Observatory

Publisher
European Audiovisual Observatory
76, allée de la Robertsau, 67000 Strasbourg, France
Tel.: +33 (0)3 90 21 60 00
Fax: +33 (0)3 90 21 60 19
iris.obs@coe.int
www.obs.coe.int

Cover layout – ALTRAN, France

Please quote this publication as
Cabrera Blázquez F.J., Cappello M., Fontaine G., Rabie I., Valais S., *The legal framework for video-sharing platforms*, IRIS *Plus*, European Audiovisual Observatory, Strasbourg, 2018

The legal framework for video-sharing platforms

Francisco Javier Cabrera Blázquez, Maja Cappello, Gilles Fontaine, Ismail Rabie, Sophie Valais

European Audiovisual Observatory

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Foreword

"Platform" is a good example of a word whose meaning has evolved over time from having a material dimension – raised structure with a flat surface (from the 16th century French word "plate-forme"), to being used in an abstract, ideological context – opportunities to view opinions (discussion platforms). Then came satellites, turning the platform into a sophisticated launch structure, followed by the explosion of Internet-based applications, which has now led to it also being used to indicate web 2.0 interaction spaces – basically covering any kind of service that can be provided through information society networks, including taxis, accommodation, phone calls, file-sharing etc.

When the web is used to share and/or distribute video files, audiovisual regulation is implicated from different angles, and one can observe a certain variety of approaches: services such as YouTube are qualified as "video-sharing platforms" (in the Audiovisual Media Service Directive currently under revision), whereas in other contexts they are simply referred to as "video platforms" (EU Court of justice in the recent Peugeot case) or "digital platforms" (in the French proposals concerning media chronology which have just been presented, and in a recently released Italian report on news consumption). At the same time, services such as Facebook, which increasingly contain audiovisual content shared by users, are called "social media". And when looking at the latest documents published by the European institutions, there seems to be a tendency to stick to just "online" – as in the Council of Europe and OSCE Recommendation on Internet freedom, in the EU Recommendation on tackling illegal content online, or in the EU Regulation on geo-blocking.

In light of this variety of definitions, and of the subsequent implications concerning the applicable legal framework (is it the AVMS Directive? or the e-Commerce Directive? and what about the Information Society Directive?) this IRIS *Plus* attempts to provide an overview of the state of the art of current legislation at European and national level, including the latest regulatory initiatives, and of the most recent developments when it comes to the case law of courts and other bodies, while at the same time outlining the self-regulatory initiatives of the industry.

Strasbourg, May 2018

Maja Cappello
IRIS Coordinator
Head of the Department for Legal Information
European Audiovisual Observatory

Executive summary

Video-sharing platforms (VSPs) and social media increasingly contribute to the cultural and economic development of the digital society. They enable individuals to unveil their creativity and be socially active by allowing them to disseminate audiovisual content and share it with other Internet users. They also open new opportunities for developing and creating businesses in the fields of communication, advertising and entertainment, including new alternatives to more traditional ways of conducting business. The services they provide are often of different types, and the platforms themselves are frequently of a hybrid nature. **Chapter 1** sets the scene and explores the market realities concerning online platforms as part of the audiovisual ecosystem.

As per the current regulatory framework, VSPs do not fall under the Audiovisual Media Services Directive (AVMSD), since they do not qualify as audiovisual media services; in fact, they qualify as Internet service providers (ISPs) under the e-Commerce Directive (ECD), which is the legal text of reference covering VSPs, alongside other information society services. The ECD envisages a limited liability regime for ISPs, which applies only when they do not have actual knowledge of illegal activity or information, or when they promptly remove the litigious content after obtaining such knowledge. As providers of services to consumers and "traders", VSPs are also affected by other transversal directives, such as the Unfair Commercial Practices Directive (UCPD), which contains provisions on transparency and professional diligence requirements in order to guarantee consumer protection. Additionally, the business models of VSPs, based on the use of their users' private data and on algorithms, have given rise to a number of new issues with regard to fundamental rights, such as the protection of human dignity, the respect for privacy and family life, the protection of personal data, and the freedom of expression and information, which are protected under EU primary legislation and by the Charter of Fundamental Rights of the European Union. **Chapter 2** gives an overview of the current applicable legal framework.

From a market perspective, these services compete to a certain extent with audiovisual media services, both directly and indirectly: directly, because they both distribute audiovisual content; and indirectly, by competing for advertising and sponsorship revenues. Despite sharing certain characteristics with audiovisual media services, VSPs are not subject to the same obligations as audiovisual media services, such as, for example, the requirement to financially contribute to the production of European works or to protect against harmful content online. Hence, in order to ensure a level playing field for all actors and a sufficient degree of protection online, the question of whether and how to adapt the current legal framework has emerged at various levels.

At national level, some EU member states are beginning to consider the need to regulate VSPs more strictly. For example, Germany, France, Italy, and the United Kingdom have tackled the question of disinformation online, and some proposed laws are being discussed; France and Germany have adopted specific rules obliging VSPs to contribute to the financial ecosystem of the audiovisual sector; and the United Kingdom has introduced

legislative measures aimed at protecting minors online. Such initiatives, together with other examples, are detailed under **Chapter 3**.

At the same time, the online industry is also directly engaged in setting up self-regulatory actions. Major VSPs and social media networks have developed their own guidelines, mechanisms and tools to empower and protect different categories of users, namely minors, consumers and rightsholders, from harmful or illegal content such as content impairing minors; disinformation; hate speech; copyright-infringing content; and unlawful commercial practices. Such initiatives are often carried out in close cooperation with national authorities, civil society and other relevant stakeholders. An overview of the most significant initiatives is presented in **Chapter 4**.

Online platforms also generate a number of new interpretative issues for the judges; these cover a variety of topics ranging from copyright and data protection to the protection of citizens, minors and consumers. **Chapter 5** provides a selection of relevant case law from the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), as well as from national courts and competent competition or regulatory authorities. It provides some insights into the interpretation of the main principles and notions related to this domain, such as the definitions of "intermediaries", "VSPs" and "audiovisual media services"; the scope of the limited liability regime applicable to information society services; the notion of an "active" or "passive" service provider, etc.

As these services are developing, there are also on-going legislative updates at European level. The European Commission's Digital Single Market (DSM) Strategy for Europe is introducing significant changes with the aim of modernising the European legal framework. Under this umbrella, the AVMSD is undergoing a significant revision process, with the introduction of a new definition for "video-sharing platform services", distinct from "audiovisual media services". A new set of obligations is proposed, aimed at protecting minors and citizens from harmful content in VSPs, through the establishment of appropriate measures and tools by these services. In the different context of the Information Society Directive, initiatives have been taken in order to impose upon information society services the obligation to prevent the availability of copyright-infringing content through their services once it has been identified as such by rightsholders. These legal initiatives, along with others, are detailed under **Chapter 6**. A table showing what stage the AVMSD interinstitutional negotiation "trilogues" are currently at is annexed under **Chapter 7**.

Table of contents

Tables

1 Setting the scene

1.1 Content available from video-sharing platforms and social media and their economic impact

1.1.1 Offerings and hybrid operators

1.1.1.1 Video-sharing platforms

Video-sharing platforms, of which YouTube and Dailymotion[1] are the two main examples, have long been the only services that enable Internet surfers to make their videos available to a user community. Their principal features are: open access for all; the lack of platform involvement in the choice of content published; the algorithmic or human curation of content; funding through advertising; and ex-post checks on the initiative of rightsholders or the platform itself. Video-sharing platforms have, with varying degrees of success, established functions that may be described as "social". For example, Google, the owner of YouTube, has sought to integrate its social network Google+ into the platform. Not long ago (2017), it launched the "YouTube communities" function to facilitate the networking of creators and their devotees. Most platforms also allow videos to be published on third-party social networks.

More recently, social networks have either added video to their offering of content shared among members of the same group (Facebook, Snapchat, Instagram) or have developed on the basis of the very concept of video-sharing (Periscope, BIGO, Live.me, Twitch). While videos were originally published in the form of links to video-sharing platforms, they are increasingly being made available on the servers of the social networks themselves.

The two categories of service remain distinct with regard to their main objective: on the one hand, video-sharing platforms with social features; on the other hand, social networks that, in particular, enable videos to be shared. However, they may, to a certain extent, be considered as belonging to the same market:

[1] See below for details of the recent development of the Dailymotion offering.

- From the point of view of consumers, who may find in them comparable videos (such as video clips or user-generated content);
- From the point of view of creators, for whom these different video-sharing platforms may constitute alternatives for content distribution;
- From the point of view of the business model, with the different platforms competing on the same advertising market.

1.1.1.2 From user-generated to professional content

The concept of "user-generated content"[2] is closely linked to that of a video-sharing platform. Theoretically, these platforms are mainly used to make personal content available, but the range of videos provided by platforms extends far beyond such content.

- While some of the material has actually been created by users, they have also been able to make content available that has, for example, been recorded from a third-party source (such as a television channel).
- The various video platforms try to encourage the emergence of "creators", that is to say, producers who, having achieved a certain level of acclaim, supply specific original content on an on-going basis and have entered into general agreements with the platforms. These agreements include the following arrangements in particular:
    - Producers given access to a proportion of the advertising revenues generated by their videos,[3] perhaps coupled with a guaranteed minimum;
    - Promotional activities;
    - Technical support in the form of training or the provision of materiel (YouTube Space);
    - The ability to post more videos on the platform, for example via a paid account.[4]
- Programmes produced by traditional media players, whether it be to benefit from a new release window, to distribute content that was originally produced for the cinema but which did not manage to secure theatrical distribution, or to produce programmes designed for or adapted to content-sharing platforms.[5]

Given the limited data available, it is impossible to determine the volume of these different types of content as a proportion of the platform catalogues or their share of total usage, but it may be noted that no payment is made for purely user-generated content in

[2] User-generated content, also known as user-created content, comprises blogs, "wikis", discussion forums, messages (posts, chats, tweets, podcasting, digital images, videos, audio files, advertisements and other forms of media created by users of an online system or service, often made available via social media websites. For more details, see for example, Katsarova, I., EPRS, European Parliamentary Research Service, "The Audiovisual Media Service Directive", EU Legislation in Progress briefing, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/583859/EPRS_BRI%282016%29583859_EN.pdf.

[3] See for example the YouTube, Facebook or Dailymotion terms of service.

[4] See for example the Vimeo terms of service.

[5] Not mentioned here is the promotional content extensively present on video platforms.

the form of a share of advertising revenues. The other content categories, either semi-professional or professional, accordingly receive the bulk of the revenues that are remitted by the platforms to producers or rightsholders. Moreover, the various services that offer video-sharing functions seem to be increasingly placing the emphasis on content supplied by "creators" or media groups. For example, Dailymotion appears to have limited its service to such content. Facebook Watch also prioritises these types of content.

1.1.1.3 Blurred borderlines between audiovisual media services

Apart from the close collaboration of video platforms with a small number of suppliers that make their content available, initiatives have been taken by some platforms to acquire rights based on a model that appears similar to that employed by audiovisual media services. For example, YouTube (in the case of its YouTube Red service) and Facebook (in the case of its Watch section) have funded a limited number of programmes on variable financial terms. The primary aim of these investments might be to increase the traffic on YouTube Red and Facebook Watch in order to persuade creators (including media groups) to produce exclusive content for the service, paid for in the form of revenue-sharing,[6] so they do not necessarily indicate a development towards a media service in the traditional sense of the term. However, platforms would then become players on the content production and audiovisual rights exploitation market on the basis of different business models.

Other examples of hybridisation between video-sharing platforms, social media and audiovisual media services may be cited: YouTube offers a direct service for purchasing films on demand that differs from the one provided by GooglePlay, although both services are operated by Google.

On the other hand, some audiovisual media services may make themselves available for the publication of content produced by third parties and do so without making any individual selections. For example, Amazon Video Direct enables rightsholders to include their programmes either within Amazon Video (a service mainly based on transactional video on demand)[7] or even within Amazon Prime (a subscription video-on-demand service). Rightsholders are not paid by purchasing rights from them but on a revenue-sharing basis.[8]

Finally, mention may be made of the role of distributors of audiovisual services that can be played by some video-sharing platforms, especially YouTube, which offers a

---

[6] Techcrunch: "Facebook launches Watch tab of original video shows", 09/08/2017, https://techcrunch.com/2017/08/09/facebook-watch/.

[7] Based on a model analogous to book-publishing services, either direct (Amazon Direct Publishing, a service offered to publishing houses) or in the form of self-publishing (Amazon Self-Publishing, a service offered to authors).

[8] The press has reported on the launch of a video-sharing service by Amazon, but the firm has yet to confirm this information. See "Amazon filed for 'AmazonTube' trademark after Google pulled YouTube from the Echo Show", Techcrunch, 20 December 2017, https://techcrunch.com/2017/12/20/amazon-filed-for-amazontube-trademark-after-google-pulled-youtube-from-the-echo-show/.

pay-TV service in the United States under the YouTube TV brand. The consumer can subscribe to a selection of channels, which, incidentally, are also available as part of the services offered by traditional distributors.

1.1.2 The difficulty in estimating the size of the audience generated by video-sharing

Data abounds on the number of users of both video-sharing platforms and social media, as well as on the number of videos consumed on those platforms. This reflects the regular use of these platforms by a considerable proportion of web users.[9] It is a more complex task to compare and contrast their audience with that of other audiovisual services, either linear or on-demand. In the online services sector, only partial use is made of time spent as a means of measurement, which is the main indicator in the audiovisual field. Moreover, the indicators are sometimes flawed: the time spent watching television is compared with time spent on the Internet, whether or not the latter is taken up with watching videos. The time devoted to looking at videos on the Internet covers programmes of a diverse nature and from very diverse sources: catch-up TV on TV channel websites; subscription video-on-demand services; video-sharing sites, etc. – calculating the amount of time spent watching videos varies according to the website. Finally, the data on the different devices that enable everyone to access online video (PCs, mobile telephones, smart TVs, etc.) are not necessarily merged.

In a report published in 2015,[10] the European Audiovisual Observatory estimated, on the basis of data from 2014 relating to certain European countries, that, depending on the country, the time spent watching any type of video online on a computer was between 5 and 10% of the total time spent watching video[11]. According to Nielsen, in the first quarter of 2017, the total time spent watching video on a computer or mobile device in the United States was about 8% of the total time devoted to watching video[12]. However, as pointed out above, the videos concerned were not only those available on video-sharing platforms and social media.

In its "Digital Day" study,[13] the British regulator Ofcom adopts a more in-depth approach that enables us to identify not only the devices used but also the categories of videos watched. According to this research, the "online video clips" category accounts for about 3% of the total time spent watching videos[14] for viewers aged 16 and over, but 21%

[9] For example, YouTube claims to have 1.5 billion logged-in users a month: https://techcrunch.com/2017/06/22/youtube-has-1-5-billion-logged-in-monthly-users-watching-a-ton-of-mobile-video/.
[10] Fontaine, G., Grece C., "Measurement of fragmented audiences", European Audiovisual Observatory, November 2015, https://rm.coe.int/16807835c0.
[11] Apart from DVD and Blu-ray.
[12] Apart from DVD and Blu-ray.
[13] https://www.ofcom.org.uk/research-and-data/multi-sector-research/general-communications/digital-day.
[14] Apart from DVD and Blu-ray.

in the case of 6 to 15-year-olds. The latter figure can be explained both by the increased use of sharing platforms by teenagers and by their lower consumption on traditional TV sets.

On the basis of these limited figures, it may be said that the consumption of programmes specific to video-sharing platforms is, on average, still low compared with television – both linear and non-linear TV – or the new video-on-demand services, especially subscription services. However, the use of these platforms by young consumers may herald a rapid increase in their importance.

1.1.3 The economic impact of video-sharing platforms and social media

Assessing the platforms' audience size is difficult enough, but it is even harder to determine their share of the advertising market. It is necessary to establish which advertising market to consider. An initial approach may be to bear in mind that it is the relatively recent use of video advertising that has enabled video content to be monetised on video-sharing platforms. This approach is based on the hypothesis that video advertising now enables online services (especially video-sharing services) to offer a real alternative to TV-screen advertising.

This approach is not entirely satisfactory because the videos offered by video-sharing platforms (like those offered by other websites in general) are not exclusively monetised in the form of video advertisements. On the other hand, video advertisements can be inserted into non-video content.

Nonetheless, according to this approach, online video advertising was worth about 3 billion euros in Europe in 2016[15], or approximately 7.5% of video advertising (TV and Internet combined), against only 2% in 2011. While Facebook's and Google's 60% combined share of the online advertising market in the United States is similar to that in Europe and although they have the same share of the video advertising market, the advertising generated by the social media and video-sharing platforms is said to amount to some 1.8 billion euros, or 5% of video advertising (TV and Internet combined). However, this estimate can be criticised because of the equivalence posited between video content and video advertising and the fact that video contributes to the growth in traffic on websites such as social media sites, and therefore to their total advertising revenues (and not only video).

Over and above their present and future importance on the advertising market, the social media and video-sharing platforms could have a crucial impact on the very model on which the financing and exploitation of audiovisual programmes is based. By setting themselves up as a solution for universal distribution open to creators, producers or media groups, the social media and video-sharing platforms are developing a model that

[15] Source: Statista.

involves remunerating the availability of content in the form of revenue-sharing. Being only marginally involved in pre-financing, the platforms would then let producers bear the risk. In return, the latter could hope to benefit from a larger share of the revenues generated through a simplified distribution network. However, that would presuppose their having financial resources available to pre-finance the creation of original content.

1.2 The main legal challenges posed by video-sharing platforms and social media

1.2.1 The challenge of agreeing on a common legal definition

From a legal perspective, video-sharing platforms give rise to a number of new situations, questions and enforcement challenges. But one of the very first legal challenges is to agree on a common understanding of what the term video-sharing platforms actually covers. Finding a clear legal definition is indeed the first condition required to allow a proper assessment of the rights and obligations attached to these legal subjects.

In the public consultation that was launched in September 2015,[16] the European Commission firstly proposed a definition of the term "online platform", as follows:

> *"an undertaking operating in two (or multi-) sided markets, which uses the Internet to enable interactions between two or more interdependent groups of users so as to generate value for at least one of the groups".*

Among the online platforms, the European Commission further distinguished between "audiovisual and music" platforms (giving examples such as Deezer, Spotify, Netflix, and Apple TV), video-sharing platforms (for example, YouTube and Dailymotion) and social networks (for example, Facebook, LinkedIn, Twitter, and Tuenti), expressly excluding Internet access providers from the scope of the definition.

This classification, however, is not crystal clear, as some of the services given as examples by the European Commission are considered as "audiovisual media services" from a legal point of view and, as such, fall under a different legal framework from that of information society services,[17] which includes a set of specific obligations attached (for

[16] Commission consultation on the Regulatory Environment for Platforms, Online Intermediaries, Data, Cloud Computing and the Collaborative Economy, 24 September 2015 to 6 January 2016, https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud.

[17] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0013.

instance, the protection of minors, the promotion of European works, advertising, etc.). On the other hand, the dividing line between some online providers of entertainment content and platforms such as YouTube offering access to content that may be produced by internet users as well as by media outlet is not always easy to determine, as mentioned earlier.

This initial definition provided by the European Commission was, by the way, contested by the majority of the respondents to the public consultation,[18] who considered it to be both too broad and too narrow. Industry stakeholders reflected the concern that regulation could be based on "platform status", and suggested instead that the focus be placed on online platform activities and business models in order to ensure coherence and a level playing-field, enforce existing regulations, and clarify the fields of application. For the majority of respondents, there cannot be a "one-size-fits-all" definition without risking an overlap with the definition of online intermediary and information society service providers. The proposed differentiation within "platforms" included platforms operating as B2B v. B2C v. C2C; platforms that function as a "passive conduit" versus those more "active" or with "editorial roles".[19]

In the Communication[20] that followed the public consultation, and in the Staff Working Document[21] that accompanied it, the European Commission came to the conclusion that *"there is no consensus on a single definition of online platforms as a clear-cut definition would likely be too narrow, or conversely apply to a very wide range of Internet services"*. The Commission instead provided for a list of five *"important and specific characteristics"* shared by online platforms, in particular:

- The ability to create and shape new markets, to challenge traditional ones, and to organise new forms of participation or conduct business based on the collection, processing, and editing of large amounts of data;
- The ability to operate in multisided markets but with varying degrees of control over direct interactions between groups of users;
- The ability to benefit from "network effects", where the value of the service increases with the number of users;
- The capacity to rely on information and communications technologies to reach users, instantly and effortlessly;
- The capacity to play a key role in digital value creation, notably by capturing significant value (including through data accumulation), facilitating new business ventures, and creating new strategic dependencies.

[18] Online Platforms Public Consultation Synopsis Report, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15877.
[19] See Chapter 5 of this publication.
[20] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe", COM(216) 288 final, Brussels, 25 May 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0288&from=EN.
[21] Commission Staff Working Document on Online Platforms, https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-online-platforms.

Among the online platforms and business models identified, in the Communication the European Commission differentiated between:

- Market places and e-commerce platforms;
- Mobile ecosystems and application distribution platforms;
- Internet search services;
- Social media and content platforms;
- Online advertising platforms.

While recognising that no general definition of "social media" platforms exists, the Commission referred to a definition provided in the Facebook/WhatsApp merger decision,[22] where it described social networking services as *"services which enable users to connect, share, communicate and express themselves online or through a mobile app"*.

The Commission jointly addressed social media platforms and "creative content outlets", as it considered both services to have the same characteristics, namely, they both allow social interactions and often offer a layer of services (including communications services, the sharing of user-generated content and the serving of advertisements) and it included some examples thereof (Facebook, Twitter, Instagram, Google+, MySpace, Pinterest, Snapchat, YouTube, Soundcloud, Origin, Wordpress and Whatsapp).

In the proposal for a revised Directive on audiovisual media services (AVMSD)[23] adopted in May 2016, the Commission defined "video-sharing platform services" as follows:

- The service consists of the storage of a large amount of programmes or user-generated videos, for which the video-sharing platform provider does not have editorial responsibility;
- The organisation of the stored content is determined by the provider of the service including by automatic means or algorithms, in particular by hosting, displaying, tagging and sequencing;
- The principal purpose of the service, or a dissociable section thereof, is devoted to providing programmes and user-generated videos to the general public in order to inform, entertain or educate;
- The service is made available by electronic communications networks.

The definition issue may become more pressing in light of the on-going debates about the question of whether to adopt additional sector-specific regulation for video-sharing platforms and social media on top of the main EU rules already applicable to

[22] Case No. COMP/M.7217 – Facebook/WhatsApp, 3 October 2014, paragraph 46, http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.

[23] Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016) 287 final, Brussels, 25 May 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0287&from=EN.

them (market freedoms, competition law, consumer protection, the protection of personal data, etc.).[24]

1.2.2 The challenges of territoriality and enforcement

The global perspective and scope of online platforms in general, including video-sharing platforms and social media, poses a challenge to national laws, which are inherently territorial in nature. This concerns in particular the enforcement of protective laws (labour law, consumer law, copyright law or privacy law), but also tax laws, where diverging rules and case law at national level makes it more difficult to adopt a common global approach and leaves the door open to "forum shopping" practices.

An example of this is offered by some major platforms, typically US-based companies, which use legal engineering to minimise their tax burden, relying on complex base erosion and profit shifting strategies, which have been the object of legal disputes with EU governments for many years now.[25]

1.2.3 The challenges on competition law

Although a regulatory response is easier in fields where there is EU competence and authority (DG Competition), competition law is being challenged by online platforms at many levels. In terms of market access, for example, regulations for operating services at national level may need to be adapted to take into account the specificities of video sharing platforms and social media and of the "sharing economy". Furthermore, to be able to enforce competition law, more importance must be attached to the market power of such platforms, given their multi-sided nature, and the relevant market where they operate must be correctly assessed. This involves, upstream, the relation between the platform and its users, through the offer of free services in exchange for the collection of data originated on the basis of the free input of platform users; and, downstream, the relation between the platform and advertisers.

As highlighted by the German Monopolkommission in its report on the challenge of digital markets,[26] from an antitrust perspective, the potential abuse by social networks can be relevant in two ways: firstly, such platforms may foreclose competitors, for

[24] See also *A. Strowel,* "Digital Platforms: To Regulate or Not To Regulate? Message to Regulators: Fix the Economics First, Then Focus on the Right Regulation", p. 2, http://ec.europa.eu/information_society/newsroom/image/document/2016-7/uclouvain_et_universit_saint_louis_14044.pdf.

[25] https://www.reuters.com/article/us-france-amazon-tax/amazon-settles-tax-row-with-france-value-undisclosed-idUSKBN1FP1FU.

[26] Monopolkommission, Competition policy (Germany): "The challenges of digital markets", Special report No. 68, July 2015, http://www.monopolkommission.de/index.php/en/press-releases/52-competition-policy-the-challenge-of-digital-markets.

instance by hindering other companies from providing services to users, or by extending their services in an anticompetitive manner; secondly, when such platforms collect data excessively and curb the users' ability to limit this data collection, this too could potentially constitute abuse.

Furthermore, video-sharing platforms providing audiovisual content are subject to different regulation than that applicable to traditional media (for example, in relation to the protection of minors, advertising or the promotion of European works), which may potentially increase the risk of competition distortions to the detriment of traditional media when such platforms are active on the same market.

Other questions also arise, which, although not typically legal ones, are relevant for the overall audiovisual ecosystem, such as how to make all actors contribute to the offer of content and to the objective of cultural diversity, and how to create a level playing field.

1.2.4 The legal challenges on fundamental rights

Video-sharing platforms and social media raise more concerns in relation to fundamental rights than any other types of e-commerce platforms due to their specific role in transmitting and displaying audiovisual content digitally and their potential impact on the users' opinion-forming process. In this regard, the state has a role to play in guaranteeing that pluralism, access to information and cultural diversity are safeguarded on these platforms.

Audiovisual content transmitted through video-sharing platforms and social media broadens the sources of information and entertainment for users to include all content that matches their preferences, relying to a large extent on complex automated decision-process systems based on algorithms that filter content in order to personalise recommendations to users. Algorithms facilitate the collection, processing and repurposing of vast amounts of data and images.[27] They are used in the online tracking and profiling of individuals whose browsing patterns are recorded by "cookies" and similar technologies such as fingerprinting, aggregated with search queries. Moreover, behavioural data is processed from smart devices, such as location and other sensor data through apps on mobile devices, presenting even more challenges for privacy and data protection. Algorithms raise general concerns because of their opacity and unpredictability. As highlighted by the Committee of experts on internet intermediaries (MSI-NET) of the Council of Europe, more transparency, accountability and some ethical

[27] In addition, it is worth noting that data related to audiovisual content consumption have a very strong identity function. The algorithms that process this data are numerous and varied: recommendation engines, programmatic advertising, etc.

standards would be desirable in their use, in the absence of any normative framework in this field.[28]

In fact, besides their direct impact on the right to privacy and data protection, algorithms also point to complex challenges for society as a whole on how to safeguard fundamental rights and human dignity in the face of rapidly changing technology, including the right to freedom of expression (which embraces the right to receive and impart information), the right to free elections, to a fair trial, the rule of law, etc. For example, following the terrorist attacks in Europe and the United States, politicians called for online social media platforms to use their algorithms for national security concerns to identify accounts that generate extremist content and to track potential terrorists. The use of algorithms in such circumstances may be justified for national security reasons, but it also raises some specific concerns related to fair trial standards (the presumption of innocence, the principle of equality, etc.) that need to be addressed.

In addition, the use of algorithms raises new specific challenges in relation to access to content and pluralism of information. In fact, video-sharing platforms and social media, just like traditional media, transmit audiovisual content to users, allowing them to form an opinion without the editorial control that is characteristic of traditional media. Just like traditional media, video-sharing platforms and social media operate according to economic principles; however, contrary to traditional media, the orientation towards user preferences is an integral part of their business model, as the services in question are mainly financed by advertising. Moving towards user preferences increases the likelihood that users will become aware of the content on offer, and that advertising can also be placed according to their preferences ("targeted advertising").[29] In this context, the concern for pluralism of and access to information is being raised by such platforms, as users may be unaware of the connection between the content that is displayed and the advertising and lucrative purposes behind it.

Finally, the use of algorithms by video-sharing platforms and social media raises important questions in relation to cultural diversity.[30] On the one hand, it may contribute to diversity by facilitating the discovery of audiovisual works that are not otherwise programmed because of their low budget, or because of the absence of a distributor or a promotional budget. Thus, thanks to the recommendation engines, some films can find an audience even if they are not programmed by conventional distribution channels. On the other hand, these algorithms can also have the opposite effect, confining individuals to personalising services according to their tastes and opinions. If this were the case, it

[28] See "Study on the human rights dimension of automated data processing (in particular algorithms) and possible regulatory implications", Committee of Experts on Internet Intermediaries, MSI-NET(2016)06, Council of Europe, https://rm.coe.int/study-on-algorithmes-final-version/1680770cbc.

[29] See also, Monopolkommission, Competition policy (Germany): "The challenges of digital markets", op. cit.

[30] See CSA Lab, "le rôle des données et des algorithmes dans l'accès aux contenus", " Les mutations de la mise à disposition de contenus audiovisuels à l'ère du numérique: conséquences et enjeux, Rapport 1 ", January 2017, http://www.csa.fr/Etudes-et-publications/Les-etudes-thematiques-et-les-etudes-d-impact/Les-publications-du-CSA-Lab/Les-mutations-de-la-mise-a-disposition-de-contenus-audiovisuels-a-l-ere-du-numerique-consequences-et-enjeux-Le-role-des-donnees-et-des-algorithmes-dans-l-acces-aux-contenus.

would potentially undermine free choice, homogenise information and polarise content around dominant visions contrary to the objective of cultural diversity.

Beyond the algorithms themselves, the use of semi-automated or automated processes for content filtering and of content removal processes by video-sharing platforms and social media may have an impact on freedom of expression and raise rule of law concerns in terms of legality, legitimacy and proportionality.[31] In addition, the automated filtering mechanisms and other tools put in place by Facebook and YouTube to remove extremist videos raise further concerns about the criteria used to determine which videos are "extremist" or show "clearly illegal content", raising the issue of "private censorship". Contrary to the intervention of public authorities in this field, private actors are not bound by the control of the constitutionality of their actions. One could argue that, at the end of the day, it is a private contractual relationship between video-sharing platforms and users and that users are fully aware of the rules of the game before they upload their videos.

These are only a few examples of the new questions that are being raised by video-sharing platforms and social media and that are at the heart of lively discussions at national and European Union level among governments and civil society.

[31] See for example, *"Facebook removes image of Copenhague's little mermaid statute for breaking nudity rules*", http://www.independent.co.uk/life-style/gadgets-and-tech/news/little-mermaid-copenhagen-denmark-removed-by-facebook-nudity-rules-a6799046.html.

2 International and EU legal framework

2.1 Council of Europe

2.1.1 Standard-setting activity related to the online environment

The Council of Europe aims to ensure that the Internet provides a safe and open environment where freedom of expression, freedom of assembly, diversity, culture, education and knowledge can flourish. To achieve this goal, the organisation has created international conventions in fields such as cybercrime, personal data protection and the protection of children. It also develops model legislation – via recommendations to its member states – and guidelines for private sector Internet actors.

The key pillar for the protection of human rights online is the European Convention on Human Rights (ECHR).[32] The European Court of Human Rights,[33] which rules on applications alleging violations of the Convention, has delivered a number of judgments concerning the right to freedom of expression and access to information, and the right to privacy, which have an impact on the online environment.[34]

The Committee of Ministers,[35] the Council of Europe's decision-making body, has, in recent years, made several recommendations addressed to member states in relation to freedom of expression and human rights on Internet platforms:[36]

- Recommendation CM/Rec(2016)5 on Internet freedom;[37]

[32] European Convention on Human Rights and its Protocols, http://echr.coe.int/Pages/home.aspx?p=basictexts&c=#n1359128122487_pointer.
[33] http://echr.coe.int/Pages/home.aspx?p=home.
[34] See Chapter 5 of this publication. See also Voorhoof D. et al and McGonagle T. (Ed. Sup.), Freedom of Expression, the Media and Journalists: Case-law of the European Court of Human Rights, IRIS themes, European Audiovisual Observatory, Strasbourg, 2016, http://www.obs.coe.int/documents/205595/2667238/IRIS+Themes+-+Vol+III+-+2016+Edition+EN+FINAL.pdf/9d9f75ba-ddbf-476e-aa65-81108471c6c9.
[35] The Committee of Ministers is composed of the Ministers for Foreign Affairs of the 47 member States of the Council of Europe or their Permanent Representatives in Strasbourg, see: https://www.coe.int/en/web/cm/about-cm.
[36] For more information see "Recommendations and Declarations of the Committee of Ministers in the field of media and information society", https://rm.coe.int/1680645b44.

- Recommendation CM/Rec(2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality;[38]
- Recommendation CM/Rec(2015)6 on the free, transboundary flow of information on the Internet;[39]
- Recommendation CM/Rec(2014)6 on a Guide to human rights for Internet users;[40]
- Recommendation CM/Rec(2013)1 on gender equality and media;[41]
- Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines;[42]
- Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services;[43]
- Recommendation CM/Rec(2011)7 on a new notion of media;[44]
- Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling;[45]
- Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet.[46]

Also worth mentioning in this regard are the 2017 Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[47] and the 2008 Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime.[48]

2.1.2 Recommendation on the roles and responsibilities of Internet intermediaries

On 7 March 2018, the Committee of Ministers of the Council of Europe adopted a Recommendation on the roles and responsibilities of Internet intermediaries.[49] The recommendation calls on member states to provide a framework based on human rights and the rule of law that lays out the main obligations of the member states with respect

[37] https://rm.coe.int/09000016806415fa.
[38] https://rm.coe.int/09000016805c1e59.
[39] https://rm.coe.int/09000016805c3f20.
[40] https://rm.coe.int/09000016804d5b31.
[41] https://rm.coe.int/09000016805c7c7e.
[42] https://rm.coe.int/09000016805caa87.
[43] https://rm.coe.int/09000016805caa9b.
[44] https://rm.coe.int/09000016805cc2c0.
[45] https://rm.coe.int/16807096c3.
[46] https://rm.coe.int/09000016805d4a39.
[47] https://rm.coe.int/16806ebe7a.
[48] https://rm.coe.int/16802fa3ba.
[49] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies), https://rm.coe.int/0900001680790e14.

to the protection and promotion of human rights in the digital environment, and the respective responsibilities of intermediaries. The Committee of Ministers recommends that member states:

- implement the guidelines included in the recommendation when devising and implementing legislative frameworks relating to Internet intermediaries, in line with their relevant obligations under CoE legal instruments[50], and promote them in international and regional forums;
- take all necessary measures to ensure that Internet intermediaries fulfil their responsibilities to respect human rights;[51]
- in implementing the guidelines, take due account of Committee of Ministers relevant recommendations;[52]
- implement the guidelines in the understanding that they are intended to build on and reinforce the Human rights guidelines for Internet service providers;[53]
- engage in a dialogue with all relevant stakeholders with a view to sharing and discussing information and promoting the responsible use of emerging technological developments that impact the exercise and enjoyment of human rights and related legal and policy issues;
- encourage and promote the implementation of effective age- and gender-sensitive media and information literacy programmes in co-operation with all relevant stakeholders;
- regularly review the measures taken to implement this Recommendation with a view to enhancing their effectiveness.

The appended Guidelines for States on actions to be taken vis-à-vis Internet intermediaries are divided into two parts:

- Obligations of member states with respect to the protection and promotion of human rights and fundamental freedoms in the digital environment: member states should respect the principles of legality, legal certainty and transparency, provide safeguards for freedom of expression, privacy and data protection and guarantee access to an effective remedy.
- Responsibilities of Internet intermediaries with respect to human rights and fundamental freedoms that member states should aim to ensure: the guidelines stress the responsibility of Internet intermediaries in respecting human rights and fundamental freedoms as well as the principles of transparency and

[50] The Recommendation mentions the European Convention on Human Rights, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Convention on Cybercrime, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence.
[51] In line with the United Nations Guiding Principles on Business and Human Rights and the Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business.
[52] See Section 2.1.1. of this publication.
[53] https://rm.coe.int/16805a39d5.

accountability. They also contain rules on the use of personal data and access to an effective remedy.

With regard to content moderation, the rights of users to receive, produce and impart information, opinions and ideas are paramount. Accordingly, any measures taken to restrict access (including blocking or removing content) as a result of a member state order or request should be implemented using the least restrictive means. When intermediaries restrict access to content in line with their own content-restriction policies, they should do so in a transparent and non-discriminatory manner; the restriction is to be implemented using the least restrictive technical means and be limited in scope and duration to what is strictly necessary to avoid the collateral restriction or removal of legal content. Any restriction of content should be limited in scope to the precise remit of the order or request and should be accompanied by information to the public, explaining which content has been restricted and on what legal basis. Notice should also be given to the user and other affected parties, unless this interferes with on-going law-enforcement activities.

The guidelines are sceptical about the use of automated means of content identification in order to prevent the reappearance of specific items of previously restricted content. Intermediaries should carefully assess its human rights impact and should ensure human review where appropriate, taking into account the risk of an over-restrictive or too lenient approach resulting from inexact algorithmic systems, and the effect these algorithms may have on the services that they provide for public debate. Restrictions of access to identical content should not prevent the legitimate use of such content in other contexts.

2.2 EU legal framework

2.2.1 Different regulation for different services?

EU law regulates the provision of audiovisual content via electronic communications networks mainly through two different legal frameworks. On the one hand, the Audiovisual Media Service Directive (AVMSD)[54] aims at the application of specific rules to services (TV broadcasting and VoD services) that fulfil certain characteristics, notably the editorial responsibility of the service.[55] On the other hand, the Electronic Commerce

[54] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010L0013&from=EN.

[55] See Section 2.2.1.2 of this publication. For further information on the material scope of the AVMSD see Cabrera Blázquez F.J., Cappello M., Fontaine G., Valais S., On-demand services and the material scope of the

Directive (e-Commerce Directive or ECD)[56] covers virtually everything else, including, among other things, video-sharing platforms and social media.[57]

The inclusion of audiovisual services available on-demand under the legal framework of the AVMSD seemed to be a major achievement when the directive was adopted in 2007. This inclusive solution solved the tension between the two sides of audiovisual regulation, according to which:

- "television broadcasting" fell under the regulatory framework established by the Television without Frontiers Directive (89/552/EEC)[58];
- "video-on-demand" was caught under the e-Commerce Directive (2000/31/EC) via the reference to the definition of "information society services" within the meaning of Article 1(2) of Directive 98/34/EC[59] as amended by Directive 98/48/EC[60].

This two-layer approach was expressed through disconnection clauses, which clearly separated the two regulatory frameworks: television broadcasting was not qualified as an information society service because it was not provided at individual request, whereas VoD, which was transmitted point to point, qualified as an information society service.

This exact same two-sided approach came to an end in 2007 with the adoption of the AVMSD, which included on-demand services in its scope, although it imposed a lesser degree of regulation on these types of services, and explicitly stated that in the event of a conflict with a provision of the ECD, the AVMSD should prevail. The new two-layer approach saw the following regulatory distribution:

- an on-demand service that is TV-like and that falls under the editorial responsibility of a media provider is regulated by the AVMSD;

AVMSD, IRIS Plus, European Audiovisual Observatory, Strasbourg, 2016, https://rm.coe.int/1680783488. See also Cabrera Blázquez F.J., On-demand Services: Made in the Likeness of TV?, in IRIS plus 2013-4, European Audiovisual Observatory, Strasbourg, 2013, https://rm.coe.int/1680783beb.

[56] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 17/2000, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN.

[57] See Cabrera Blázquez F.J., User-Generated Content Services and Copyright, IRIS Plus, European Audiovisual Observatory, Strasbourg, 2008, https://rm.coe.int/09000016807833f5.

[58] Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31989L0552:EN:HTML. Amended by Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31997L0036&from=en.

[59] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31998L0034&from=EN.

[60] Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31998L0048&from=EN.

- all other on-demand audiovisual content provided by Internet-based services, such as content hosted by online video-sharing platforms, social media or by any other intermediaries, continues to be qualified as an information society service and falls under the ECD.

The rationale behind the choice of regulating audiovisual media services (AVMS) and information society services (ISS) separately may originally have been necessary because of the scarcity of frequencies and in order to ensure a diversity of opinions. That is why there is a set of obligations for on-demand AVMS that does not apply to ISS. However, now that the offer of audiovisual services has developed in many different ways and that the consumption habits of the viewers have changed as well, the classification of certain services may seem unclear. This is the case, for example, with video-sharing platforms (such as YouTube, Dailymotion, etc.) or social media offering access to audiovisual content produced by different types of users, including not only private individuals but also media outlets and providers of goods and services. Moreover, beyond the issue of the classification of certain services, the notion of "Internet intermediary" and its liability regime have been called into question in recent times.[61] According to some critical voices, the distinction between editor and host does not reflect the actual responsibilities of service providers in distributing content online.[62]

2.2.2 General liability regime of video-sharing platforms and social media

The purpose of the ECD is to contribute to the proper functioning of the internal market by ensuring the free movement of ISS between the member states. It harmonises certain national provisions on ISS relating to: the internal market; the establishment of service providers; commercial communications; electronic contracts; the liability of intermediaries; codes of conduct; out-of-court dispute settlements; court actions; and cooperation between member states. This Directive complements EU law applicable to ISS without prejudice to the level of protection for, in particular, public health and consumer interests, as established by EU acts and national legislation implementing them in so far as this does not restrict the freedom to provide ISS.

Articles 12-14 of the ECD limit liability for ISS in three cases:

- mere conduit (Art. 12 ECD)[63]

[61] See, for example, Rapport d'information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par le groupe de travail sur l'évaluation de la loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon (2), Par MM. Laurent Béteille et Richard Yung, Sénateurs. p. 42 and ff. N° 296 Sénat, Session Ordinaire de 2010-2011, Enregistré à la Présidence du Sénat le 9 février 2011, https://www.senat.fr/rap/r10-296/r10-2961.pdf.

[62] See Chapters 3 and 6 of this publication for more information on this discussion.

[63] An ISS providing the transmission in a communication network of content provided for by the user of the service, or a service providing access to a communication network. Acts of mere conduit also include the

- caching (Art. 13 ECD)[64]
- hosting (Art. 14 ECD)

Video-sharing platforms and social media normally fall under the liability regime concerning hosting providers. According to Article 14 ECD, hosting is an ISS that consists of the storage of information provided by a recipient of the service. Such a service is not liable for the information stored by the user, provided that:

- the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

The limitation of liability does not apply when the user of the service acts under the authority or the control of the provider.

Notwithstanding this rule, a court or administrative authority may require a service provider to terminate or prevent an infringement if foreseen by the legal system of the member state in question. Member states may also establish procedures for the removal or disabling of access to information.

Article 15 ECD prohibits member states from imposing a general obligation on ISS to monitor the information which they transmit or store, or to request that providers actively seek out facts or circumstances indicating illegal activity.[65] Despite this general liability regime, this does not concern monitoring obligations in specific cases and, in particular, does not affect orders by national authorities in accordance with national legislation (Recital 47 ECD). Moreover, member states can require hosting providers to apply a "duty of care", as explained in Recital 48 ECD:

> *[t]his Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.*

Furthermore, the e-Commerce Directive encourages the drawing up of codes of conduct[66] at EU level and voluntary agreements among the industry, as well as so-called "Notice

---

automatic, intermediate and transient storage of the information transmitted when this takes place in order to carry out the transmission in the communication network.

[64] Caching means the automatic, intermediate and temporary storage of information in a communication network, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request.

[65] Member States are free to establish obligations for ISS providers to promptly inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements (Article 15.2 ECD).

[66] Article 16 ECD.

and take-down" (NTD) procedures[67] so that ISS can act expeditiously to remove or disable access to illegal content. This designation (also referred to as "Notice and action") usually covers the procedure according to which an intermediary takes down or prevents access to information or activity following a notice of infringement. Blocking may become the only solution when take-down is not possible because the illegal activity or information is stored in a different country from the one where the servers of the ISPs are located.

Other directives also set the basis for ISPs to play an active role in strengthening the enforcement of copyright online. This is so, for example, in the case of the Enforcement Directive,[68] which provides that member states shall ensure that rightsholders can apply for an injunction against ISPs whose services are being used by a third party to infringe IPRs (Articles 9 and 11) and which encourage the development of self-regulatory codes of conduct in this field (Article 17).[69]

2.2.3 Commercial communications in video-sharing platforms and social media

The main rules concerning commercial communications in online platforms, and therefore video-sharing platforms and social media, are contained in the e-Commerce Directive and the Unfair Commercial Practices Directive.[70]

2.2.3.1 e-Commerce Directive

Article 2(f) ECD defines commercial communications as "any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession." Excluded from this definition are:

- information allowing direct access to the activity of the company, organisation or person, like domain names or electronic-mail addresses,
- communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration.

[67] Recital 40, Article 21(2) ECD.
[68] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048R%2801%29.
[69] For more information on this topic see Cabrera Blázquez F., Cappello M., Grece C., Valais, S., "Copyright enforcement online: policies and mechanisms", IRIS Plus, European Audiovisual Observatory, Strasbourg, 2015, https://rm.coe.int/1680783480.
[70] For more information on these and other directives in the field of commercial communications see Cabrera Blázquez F.J., Cappello M., Grece C., Valais S., "Commercial communications in the AVMSD revisión", IRIS Plus, European Audiovisual Observatory, Strasbourg, 2017, https://rm.coe.int/168078348c.

Article 5 ECD lists the general information to be rendered accessible by a service provider. Moreover, Article 6 ECD enumerates the conditions that commercial communications which are part of, or constitute, an ISS shall comply with:

- the commercial communication shall be clearly identifiable as such;
- the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
- promotional offers, such as discounts, premiums and gifts, where permitted in the member state where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;
- promotional competitions or games, where permitted in the member state where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

With regard to unsolicited commercial communication by electronic mail, Article 7 ECD requires that such commercial communication "shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient."

2.2.3.2 Unfair Commercial Practices Directive

The e-Commerce Directive and relevant EU consumer *acquis* apply in principle in a complementary manner. According to its Article 1(3), the e-Commerce Directive "complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services". One of those "Community acts" dealing with consumer interests is the Unfair Commercial Practices Directive (UCPD).[71] The UCPD applies to business-to-consumer (B2C) transactions and aims at contributing "to the proper functioning of the internal market" and at achieving "a high level of consumer protection by approximating the laws, regulations and administrative provisions of the Member States on unfair commercial practices harming consumers' economic interests." (Article 1 UCPD). Commercial communications, and in particular advertising, are identified therein as a B2C commercial practice (Article 2(d) UCPD).

[71] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005L0029&from=EN.

A Commission Staff Working Document[72] provides guidance on the implementation/application of the UCPD. Video-sharing platforms are generally covered by this directive. However, given that the UCPD only applies in B2C situations, the first step in assessing whether this Directive is applicable to any given online platform provider should be to evaluate whether the service provider qualifies as a "trader" under Article 2(b) UCPD. The second step is to evaluate whether the service provider engages in "business-to-consumer commercial practices" (Article 2(d) UCPD), towards users (suppliers and recipients) who qualify as "consumers" (Article 2(a) UCPD).

The service provider of a video-sharing platform qualifying as a "trader" must comply with EU consumer and marketing law as far as its own commercial practices are concerned. Traders are subject to the transparency requirements of Articles 6 and 7 UCPD, which requires them to refrain from misleading actions and omissions whenever engaging in the promotion, sale or supply of a product to consumers. Furthermore, under Article 5(2) UCPD, no service provider qualifying as a "trader" should act contrary to the requirements of professional diligence in its commercial practices towards consumers.[73]

The professional diligence duties of traders under the UCPD are different from the liability regime of Article 14 of the e-Commerce Directive. Whenever a video-sharing platform is considered a "trader" in the sense of the UCPD (Article 2(b) UCPD) it will then be required to act with a degree of professional diligence (Article 5(2) UCPD) with regard to its specific field of activity (Article 2(h) UCPD) and not mislead its users/consumers by either action or omission (particularly with reference to Articles 6(1)(f) and 7(1) and (2) UCPD). Platforms which are considered "traders" should take appropriate measures which – without amounting to a general obligation to monitor or carry out fact-finding (see Article 15(1) e-Commerce Directive) – enable relevant third-party traders to comply with EU consumer and marketing law requirements and users to clearly understand with whom they are possibly concluding contracts.

If video-sharing platforms (and social media) falling within the scope of the UCPD fail to comply with such professional diligence requirements or otherwise promote, sell or supply a product to users in an unfair manner, they can be found in breach of EU consumer and marketing law and cannot invoke the intermediary liability exemption under the e-Commerce Directive.[74]

---

[72] Commission Staff Working Document Guidance on the implementation/application of directive 2005/29/ec on unfair commercial practices accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses (SWD/2016/0163 final), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0163&from=EN.

[73] 'Professional diligence' means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity (Article 2(h) UCPD).

[74] See Chapter 5 of this publication for more information on case law concerning the liability regime of Internet intermediaries.

2.2.4 Protection of minors and human dignity in online platforms

At EU level, the protection of minors in the media environment has been debated for many years. It has become a recurrent topic in recent times, with the convergence of digital technologies and the increasing use of mobile devices by children, including on-demand media services on the Internet and online video games. The ways to limit and prohibit the spread of illicit and harmful media content in relation to young people requires the EU regulator to find a delicate balance between different fundamental rights and to put in place appropriate regulatory instruments. In particular, the content providers' right of freedom of expression should be balanced with the public-interest objective of protecting minors, which is often accompanied by control, filtering tools and some type of censorship. The question of protecting minors in audiovisual and online services has therefore been addressed at various levels of the EU legal order, from the primary legislation in the Treaty on the European Union (TEU)[75] and the Charter of Fundamental Rights of the European Union (CFREU),[76] to secondary legislation, through various directives and recommendations.

The main provision in this regard is Article 6(3) TEU on freedom of expression, which incorporates Article 10 of the ECHR into the EU legal framework. The right of expression is also included in Article 11 of the CFREU, which also incorporates fundamental freedoms of the ECHR in its Article 53. Article 24 of the CFREU addresses the rights of the child and establishes that children shall have the right to such protection and care as is necessary for their well-being and that in all actions relating to children taken by public authorities or private institutions, "the child's best interest must be a primary consideration". Finally, Article 7 of the CFREU states that everyone has the right to respect for his or her "private life, home and communication".

At the secondary legislation level, the protection of minors on audiovisual and online services has been addressed by the EU in many directives and recommendations.[77] With respect to the protection of minors in audiovisual media services, the main provisions are set out in the Audiovisual Media Services Directive (AVMSD), which establishes some minimum standards and mutual recognition in this field, covering both linear and non-linear audiovisual services. Under Article 4(8) AVMSD, all other services delivered over electronic communications networks are covered by the e-Commerce Directive, as with information society services. The e-Commerce Directive only allows member states to restrict services which "prejudice" or "present a serious and grave risk of prejudice" to the protection of minors. On the other hand, it exempts those services which are excused from responsibility under certain circumstances (for instance, mere conduits, caching and hosting services) from fulfilling obligations imposed by member states, thus

[75] Consolidated version of the Treaty on European Union, OJEU 2010/C 83/01, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2010:083:FULL&from=en.
[76] Charter of Fundamental Rights of the European Union (2010/C 83/02), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF.
[77] Issues of privacy and data protection are dealt with in section 1.1.5. of this publication.

limiting the impact of other legal instruments in the field of the protection of minors in ISS. In this context, traditional approaches are increasingly considered as having a limited effect on the regulation of the protection of young viewers, and new measures, such as self- and co-regulation and education instruments, have been gradually called for by the EU legislator as necessary complementary tools for user empowerment.[78]

2.2.4.1 Other EU initiatives in relation to the protection of minors against impairing content in a converging environment

In view of the rapid growth in the European video games market and the increasing risk of young video game users being exposed to illegal or harmful content, in 2002, the EU Council addressed the question of the protection of consumers, through the labelling of certain video and computer games according to age group,[79] promoting self-regulation as an adequate means to achieve this goal.[80]

With regard to the Internet, it is worth noting that since 1999, the European Commission has funded the "Safer Internet Programme"[81] (SIP), which aims at empowering and protecting children and young people online, and fighting illegal and harmful online content and conduct. The SIP identifies areas requiring concrete measures on which the Community resources should be focused. The 1999 Action Plan defines four specific objectives: the creation of a safer environment through a network of hotlines and the adoption of codes of conduct; the development of a filtering and rating system; the encouragement of awareness-raising actions and other supporting actions, such as the assessment of legal implications; and coordination with other similar international initiatives.

After the positive outcome of this four-year plan,[82] in 2005, the Commission proposed a new mandate for an extended Safer Internet Action Plan (the so-called IAP-

[78] See Chapter 4 of this publication for further details on self- and co-regulation in relation to the protection of minors and young people in video-sharing platforms and social media.

[79] Council Resolution on the protection of consumers, in particular young people, through the labelling of certain video and computer games according to the appropriate user age group, 2002/C 65/02, 1 March 2002, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002G0314%2801%29&from=EN.

[80] See Chapter 4 of this IRIS PLUS on self- and co-regulatory instruments.

[81] European Parliament and European Council, Decision 276/1999/EC of 25 January 1999 adopting a Multi-annual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors (OJ L 33, 6 February 1999, p.1) as amended by Decision 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 (OJ L 162, 1 July 2003, p. 1), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999D0276&from=EN.

[82] See the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions concerning the evaluation of the multi-annual community action plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content, primarily in the area of the protection of children and minors, COM (2003) 653 final, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0653&from=EN.

Plus),[83] which was again extended and broadened in 2009 to "take into account currently unknown future developments in the online environment". The 2009-2013 Action Plan[84] included actions in relation to the promotion of a safer online environment and public awareness-raising campaigns based on self-regulatory principles. These actions were framed to encompass better "user-empowerment", not only for parents and carers, but also for children and young people, and to stimulate stakeholders to take responsibility, cooperate and exchange experiences and best practices at European and international level. Moreover, the Action Plan acknowledged the need to create and build up an adequate knowledge base for addressing both existing and emerging uses, risks and consequences and for mapping both quantitative and qualitative aspects in this context. The SIP focused on the creation of a safer online environment and the fight against illegal and harmful content. It included actions such as the introduction of the Safer Internet Day[85] and the Safer Internet Centre, which support the development and implementation of codes of self-regulation and codes of conduct. The SIP was also the basis for the European Commission supporting a number of other self-regulatory initiatives in this field.

In a Communication of 2011 on "An EU Agenda for the Rights of the Child"[86], the European Commission reiterated its commitment to support member states and other stakeholders in strengthening prevention, empowerment and the participation of children in order to make the most of online technologies and to counter cyber-bullying behaviour, exposure to harmful content and other online risks, namely through the Safer Internet Programme, and in cooperation with the industry, through self-regulatory initiatives. However, an evaluation report[87] in the field of social networking services (SNS) carried out in 2010 stressed the need for improvement in terms of the effectiveness and implementation of some of these self-regulatory initiatives.

On the other hand, in 2012, the European Commission proposed a "strategy for a better Internet for children",[88] with a work programme focused on increased awareness at school, wider use of technological solutions – reporting tools, age-appropriate privacy settings, wider use of content classification, wider availability and use of parental

---

[83] Decision N° 854/2005/EC of the European Parliament and of the Council, Decision of 11 May 2005 establishing a multi-annual Community programme on promoting safer use of the Internet and new online technologies, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005D0854&from=EN.

[84] Decision N° 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communicating technologies, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D1351&from=EN.

[85] Available at https://www.saferinternetday.org/.

[86] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "An EU Agenda for the Rights of the Child", COM(2011) 60 final, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0060.

[87] Staksrud, E. and Lobe, B. (2010) Evaluation of the implementation of the Safer Social Networking Principles for the EU Part I: General Report. European Commission Safer Internet Programme, Luxembourg, https://www.duo.uio.no/bitstream/handle/10852/27216/Safer-Social-Networking-part1.pdf.

[88] Safer Internet – A multi-annual union programme on protecting children using the Internet and other communication technologies, Work Programme 2013, C(2013) 1954, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1964.

controls, etc. – and the fight against child sexual abuse, based on self-regulation. Collective results and engagements were made public, including recommendations for best practices by the biggest players in the market.

Following the adoption, in 2012, of the "European Strategy to Make the Internet a Better Place for Children", the SIP was renamed "Better Internet for Kids" (BIK). Over the years, the activities carried out under BIK have focused on raising awareness, fighting illegal content, filtering, and content labelling, through the involvement of civil society in child online safety issues and the exchange of information on the use of new technologies by young people.

The European Strategy to Make the Internet a Better Place for Children relies to a great extent on industry self-regulation to adapt rapidly to new security challenges. For example, the "Alliance to better protect minors online"[89], launched on 7 February 2017, is one of these industry initiatives. It consists in a collaborative platform through which 22 leading ICT and media companies[90] have committed to a series of actions to tackle harmful content and conducts, mainly through user-empowerment (parental and reporting tools, content classification, etc.); cooperation and the sharing of best practices; awareness raising; and the promotion of positive, educational and diversified online content. Prior to the creation of Alliance, the "CEO coalition to make Internet a better place for kids"[91] was launched in December 2011 with the aim of addressing emerging challenges and taking positive actions to put in place simple and robust reporting tools for users, as well as age-appropriate privacy settings, content classification, parental controls and effective takedown of child sexual abuse material.

As regards video-sharing platforms and social media more specifically, as early as February 2009, the major social networking services providers active in Europe – including the video-sharing platform Dailymotion – signed a self-regulatory agreement, "The European Safer Social Networking Principles",[92] through which they committed to putting in place measures to ensure the safety of minors on their services. The principles, which were developed in consultation with the European Commission and a number of NGOs, acknowledged that there was no "one-size-fits-all" solution, as platforms vary greatly in terms of services provided, business model, size, and potential risks for users. However, certain common features attached to "social networking" platforms were identified at the time, such as the possibility offered to users to have online social interaction, a personal profile page, and the option of sharing content and searching for other users through a search function. For these platforms, four main categories of content were identified as posing potential online risks to children and young people:

- "Illegal content", such as images of child abuse and unlawful hate speech;

[89] For further details, see the Statement of Purpose and the action plan, http://ec.europa.eu/newsroom/document.cfm?doc_id=42408.

[90] ASKfm, BT Group, Deutsche Telekom, Disney, Facebook, Google, KPN, The LEGO Group, Liberty Global, Microsoft, Orange, Rovio, Samsung Electronics, Sky, Spotify, Sulake, Super RTL, TIM (Telecom Italia), Telefónica, Telenor, Telia Company, Twitter, Vivendi, Vodafone.

[91] https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ceo_coalition_statement.pdf.

[92] https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf.

- "Age-inappropriate content", such as pornography or sexual content, violence, or other content with adult themes which may be inappropriate for young people.
- "Contact", which relates to inappropriate contact from adults with a sexual interest in children or by young people who solicit other young people.
- "Conduct", which relates to how young people behave online. This includes bullying or victimisation (behaviours such as spreading rumours, excluding peers from one's social group, and withdrawing friendship or acceptance) and potentially risky behaviours (which may include, for example, divulging personal information, posting sexually provocative photographs, lying about one's real age or arranging to meet face-to-face with people only ever previously met online).

To effectively tackle this content, the Principles recommended a multi-stakeholder collaboration, involving online service providers, governments, parents, teachers, users and NGOs, based around seven main principles:

- Awareness raising, through targeted guidance and educational materials;
- Age-appropriate settings;
- Users empowerment through tools and technology;
- User-friendly reporting mechanisms;
- Responsiveness to notifications of illegal content or conduct;
- Enabling users to employ a safe approach to personal information and privacy;
- Assessing the means for reviewing illegal or prohibited content/conduct.

All the European interventions in this field have a non-binding character. Moreover, they all support the development and the implementation of technical tools and, among the legal tools, they recommend mainly self-regulation as the best regulatory solution. This option is not only due to the fact that technical tools and self-regulation can have a higher level of flexibility and can better fit the needs of an ever-changing environment, but also the general argument – clearly stated in IAPs decisions – that "[r]eaching international agreement on legally binding rules is desirable but will be a challenge to achieve and, even then, will not be achieved rapidly. Even if such agreement is reached, it will not be enough in itself to ensure implementation of the rules or to ensure protection of those at risk".

2.2.4.2 Specific provisions against child pornography on the Internet

The Directive on combating the sexual abuse and sexual exploitation of children, and child pornography[93] establishes minimum rules concerning the definition of criminal offences and sanctions in the area of the sexual abuse and sexual exploitation of children, child pornography and the solicitation of children for sexual purposes. It also introduces

[93] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32011L0093&from=EN.

provisions to strengthen the prevention of those crimes and the protection of the victims thereof.

Concerning child pornography on the Internet, Article 25 of this Directive imposes on member states the obligation to take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory. Furthermore, member states may take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards must also include the possibility of judicial redress.

2.2.4.3 Specific provisions against radicalisation and terrorism recruitment on the Internet

Since the beginning of 2013, the issues of radicalisation and foreign terrorist fighters have been regular items on the agenda of the Council of the European Union and the European Council. After the terrorist attacks in Paris in January 2015, the European Union decided to reinforce its response and accelerate the implementation of agreed measures. On 12 February 2015, EU leaders held a debate on the way forward and agreed on a statement to guide the work of the European Union and the member states in the months to come. This statement[94] called for specific measures, focusing on three areas of action:

- ensuring the security of citizens
- preventing radicalisation and safeguarding values
- cooperating with international partners

Among many other measures, the European Council called for adequate measures to be taken, in accordance with national constitutions, to detect and remove Internet content promoting terrorism or extremism, including through greater cooperation between public authorities and the private sector at EU level and working with Europol to establish Internet referral capabilities.

At the European Council of June 2017,[95] EU leaders called on the industry to help combat terrorism and crime online. According to the European Council, industry has its own responsibility to help combat terrorism and crime online. Building on the work of the EU Internet Forum, the European Council expects industry to establish an Industry Forum

[94] Informal meeting of the Heads of State or Government Brussels, 12 February 2015 - Statement by the members of the European Council, http://www.consilium.europa.eu/en/press/press-releases/2015/02/12/european-council-statement-fight-against-terrorism/.

[95] European Council conclusions on security and defence, 22/06/2017, http://www.consilium.europa.eu/en/press/press-releases/2017/06/22/euco-security-defence/.

and to develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. This should be complemented by the relevant legislative measures at EU level, if necessary. The European Council also called for addressing the challenges posed by systems that allow terrorists to communicate in ways that competent authorities cannot access, including end-to-end encryption, while safeguarding the benefits these systems bring for the protection of privacy, data and communication. The European Council considers that effective access to electronic evidence is essential to combating serious crime and terrorism and that, subject to appropriate safeguards, the availability of data should be secured.

2.2.4.4 EU approach towards tackling illegal content online

The European Commission's Communication on tackling illegal content online[96] aims at increasing the proactive prevention, detection and removal of illegal content inciting to hatred, violence and terrorism online. It concerns the removal of illegal content online: incitement to terrorism, illegal hate speech, or child sexual abuse material, as well as infringements of intellectual property rights and consumer protection online. The Communication provides guidance on detecting and notifying, removing, and preventing the reappearance of such illegal content.

Concerning the detection of illegal content, online platforms should act swiftly upon binding orders or administrative decisions issued by the relevant authorities, and cooperate closely with law enforcement officials, while providing adequate safeguards for their users. This cooperation with law enforcement authorities should enable the effective enforcement of takedown requests and establish an alert system to be accessed by the authorities. To achieve this effective cooperation, online platforms should have the necessary resources to understand the legal field in which they operate and to establish points of contact in the European Union as well as technical interfaces that facilitate such cooperation. Notices issued by trusted flaggers should be fast-tracked by platforms. A trusted flagger is a specialised entity, ideally subjected to criteria based on the respect for fundamental rights, which could be part of an EU-wide standardisation framework. Users should have access to a notification system that is user-friendly, enabling sufficiently precise reports.

As regards the liability exemption provided for in Article 14 of the e-Commerce Directive, the Communication clarifies that the adoption of proactive measures by online platforms themselves, as such, should not lead to the loss of the liability exemption. Any knowledge of illegal activities or illegal information obtained from such measures, may, however, lead to a loss of the liability exemption unless the platform acts expeditiously to remove the content upon obtaining such knowledge. The Communication encourages the use and further development of automatic detection technologies.

---

[96] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online, Towards an enhanced responsibility of online platforms, COM(2017) 555 final, 28. September 2017, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=47383.

The removal of illegal content should generally happen as speedily as possible and without impediment to prosecution. Notwithstanding this, there should be robust safeguards concerning the removal of legal content. The meaning of "expeditious" removal, as defined by the e-Commerce Directive, should depend on a case-by-case examination, together with factors such as the contextual information required to determine the legality of content. The Communication suggests that in cases where serious harm is at stake, speedy removal can be subject to specific time frames. Removal times and procedures should be clearly reported in transparency reports, and evidence for criminal offences should be transmitted to law enforcement authorities. Furthermore, the content policy should be explained in the terms of service of the online platform, including information on the procedure for contesting removal decisions. The possibility of contesting such a decision should generally be available to any user whose content has been deleted, with few exceptions. The resolution of disputes by dispute settlement bodies is encouraged.

Due to the nature of the online environment, the reappearance of illegal content is extremely easy. To counter this, measures to prevent such reappearance include the suspension of repeat infringers, a database of reappearing illegal content accessible by all online platforms, and the introduction and further development of automatic re-upload filters. The latter should be subject to a reversibility safeguard and be made transparent in the platform's terms of service.

The Commission will monitor progress and assess whether additional measures are needed, including possible legislative measures, which will be completed by May 2018.

Building on the 2017 Communication and on various voluntary initiatives already undertaken by hosting service providers in their fight against illegal content online, the European Commission's Recommendation on measures to effectively tackle illegal content online[97] addresses the need for IT companies and member states to put in place a series of operational measures, for the effective removal of illegal content, as well as the need for necessary safeguards intended to protect users' fundamental rights.

The Recommendation encourages IT companies to ameliorate their notice and action procedures, allowing their users to submit sufficiently precise and adequately substantiated notices and providing fast-track procedures to process notices submitted by trusted flaggers. Content providers shall in any case be given the chance to issue counter-notices in order to avoid over-removal of content. Moreover, companies are encouraged to have a system in place which allows them to take proactive measures in respect of illegal content, but effective and appropriate safeguards shall exist which include human oversight and verification. Hosting service providers should cooperate with one another and share their best practices among each other. Under certain circumstances dealing with criminal offences, hosting providers and member states should cooperate with each other.

[97] Commission Recommendation on measures to effectively tackle illegal content online, 1 March 2018, C(2018) 1177 final, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50095.

Regarding terrorist content, hosting service providers should have fast-track procedures in place which allow them to process referrals as quickly as possible, and member states should provide their national competent authorities with the necessary resources for the effective identification and submission of referrals. Hosting service providers are also advised to take proactive measures which would ensure that previously removed terrorist content cannot be uploaded again. Moreover, cooperation among hosting providers, especially with SMEs, as well as between hosting providers and competent authorities is encouraged. It is recommended that hosting service providers remove terrorist content within one hour of being notified through referral. Importantly, both member states and hosting service providers should collaborate with the Commission, by submitting to it all relevant information, with a view to enabling the latter to monitor progress. A monitoring process of this type might give rise to additional steps which could include the proposal of binding acts of Union law.

2.2.5 Data protection and privacy

The Charter of Fundamental Rights of the European Union (CFREU)[98] includes the right to respect for everyone's private and family life, home and communications (Article 7 CFREU). It also foresees the right to the protection of personal data (Article 8 CFREU). The processing of such data must be done in a fair way for specified purposes and on the basis of the consent of the person concerned, or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

In May 2016, a new EU data protection package was adopted, which included the General Data Protection Regulation (GDPR) and the Police Directive. A new e-privacy Regulation is expected to be adopted by the end of 2018.

2.2.5.1 General Data Protection Regulation

The EU General Data Protection Regulation (GDPR)[99] replaces the Data Protection Directive[100] and aims at harmonising data protection laws across Europe. The GDPR lays down rules relating to the protection of natural persons with regard to the processing of

[98] Charter of Fundamental Rights of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[99] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[100] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

personal data and rules relating to the free movement of personal data. It protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The GDPR came into force on 24 May 2016 and will apply from 25 May 2018.

The GDPR does not affect the application of the liability rules of the e-Commerce Directive.

As regards its territorial scope (Article 3), the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller[101] or a processor[102] in the Union, regardless of whether the processing takes place in the Union or not. It also applies to the processing of the personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment from the data subject is required, to such data subjects in the Union; or
- the monitoring of their behaviour as far as their behaviour takes place within the Union.

The GDPR also applies to the processing of personal data by a controller not established in the Union, but in a place where member state law applies by virtue of public international law.

The consent of the data subject is a fundamental part of the GDPR rules. It is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 4(11) GDPR). Where processing is based on consent (Article 7 GDPR), the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data. If the consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. The data subject has the right to withdraw his or her consent at any time but it will not affect the lawfulness of processing based on consent before its withdrawal. The data subject shall be informed of the possibility of withdrawing consent prior to giving it. In any event, it must be as easy to withdraw as to give consent.

With regard to consent in relation to the offer of information society services directly to a child, the processing of a child's personal data shall be lawful where the child is at least 16 years old. Where the child is below the age of 16, such processing shall be

[101] 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (Article 4(7) GDPR).

[102] 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4(8) GDPR).

lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member states may provide by law for a lower age for those purposes but not below 13 years of age. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.[103]

Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of appropriate safeguards.[104]

Another important feature of the GDPR is the right to erasure, better known as the right to be forgotten (Article 17 GDPR). The data subject will have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Where the controller has made the personal data public, he/she will have to inform controllers that are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. Exceptions apply to the extent that processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or member state law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

[103] The GDPR rules on consent shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.
[104] See Article 46 GDPR.

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

Article 20 GDPR enshrines a right to data portability, whereby the data subject shall have the right to receive his/her personal data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance.

Article 25 GDPR imposes the so-called data protection by design and by default. The controller will have to implement measures which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR. Moreover, the controller will have to implement appropriate measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

2.2.5.2 The draft e-privacy Directive

On 10 January 2017, the European Commission adopted a proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (e-Privacy Regulation).[105] The proposed Regulation is a result of the review of the e-Privacy Directive[106] that was announced in the European Commission's Digital Single Market Strategy.

The draft Regulation will broaden the material scope of the e-privacy rules and clarify their territorial scope. It will cover the processing of "electronic communications data", which includes electronic communications content and electronic communications metadata that are not necessarily confined to personal data. Furthermore, it will be binding not only on electronic communications services providers, but also on providers of so-called "over-the-top" services and machine-to-machine communications. In addition, the territorial scope of its application will not be limited to the European Union and will apply to "electronic communications data processed in connection with the provision and use of electronic communications services in the [EU], regardless of whether or not the processing takes place in the [EU]."

---

[105] European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, 10 January 2017, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010.

[106] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058.

The proposed Regulation will expand the ability of businesses to process electronic communications metadata, such as location data. Under the new rules, the consent of the end-user will be required just once, encompassing the processing of both communications content and metadata. For the purposes of the e-Privacy Regulation, the end-user's consent will have the same meaning and will be subject to the same conditions as the data subject's consent under the GDPR.

The rules on cookies will be streamlined. In particular, the proposed Regulation clarifies that no consent would be required for cookies that are necessary for the functioning of websites, cookies that improve Internet experience or cookies that are used by a website to count the number of visitors it has. In all other cases, the processing and storage of cookies is only allowed with the consent of the end-user. The proposed rules also require Internet browsers to offer end-users the option of preventing third parties from storing cookies on their terminal equipment or processing cookies already stored on that equipment.

2.2.6 Enforcement of national laws and territoriality rules

Both the AVMSD and the e-Commerce Directive aim at contributing to the proper functioning of the internal market by ensuring the free movement of services between the member states. The country of origin principle enshrined in both directives ensures that any audiovisual media service originating from a provider established in one state can freely circulate across other states without the need for any further authorisation or for following the rules of the latter. Any attempt to restrict such circulation, as well as any imposition of further obligations on the providers with whom the audiovisual content originates, would be against this principle. Only in certain cases does the opposite apply, namely the principle of the country of destination, according to which it is up to the country where the services are delivered to determine which rules are applicable and which bodies are competent for their monitoring and enforcement.

In the case of the AVMSD, the country of origin principle is to be regarded as the core of this directive, as it is essential for the creation of an internal market and it applies to all audiovisual media services in order to ensure legal certainty for media service providers, as well as the necessary basis for new business models and the deployment of such services. It is also essential in order to ensure the free flow of information and audiovisual programmes in the internal market.[107]

The e-Commerce Directive is also based on the country of origin principle but contains a list of sectors where the principle of the country of origin is reversed in favour of the country of destination:

- copyright, neighbouring rights, rights referred to in Directive 87/54/EEC(1) and Directive 96/9/EC(2) as well as industrial property rights,

[107] See Recital 33 AVMSD.

- the emission of electronic money by institutions in respect of which member states have applied one of the derogations provided for in Article 8(1) of Directive 2000/46/EC(3),
- Article 44(2) of Directive 85/611/EEC(4),
- Article 30 and Title IV of Directive 92/49/EEC(5), Title IV of Directive 92/96/EEC(6), Articles 7 and 8 of Directive 88/357/EEC(7) and Article 4 of Directive 90/619/EEC(8),
- the freedom of the parties to choose the law applicable to their contract,
- contractual obligations concerning consumer contacts,
- formal validity of contracts creating or transferring rights in real estate where such contracts are subject to the mandatory formal requirements of the law of the member state where the real estate is situated,
- the permissibility of unsolicited commercial communications by electronic mail.

As a practical consequence of these exceptions included in the e-Commerce Directive, the issue of territoriality is treated differently according to the rights to be protected: in the case of copyright infringements, the competent member state is the country where the services are delivered, whereas in the case of content-related issues it is for the member state of establishment to intervene.

Moreover, and similar to the rules included in the AVMSD, the e-Commerce Directive contains specific procedures allowing the country of reception to restrict retransmission on its territory in case of severe violations concerning "the protection of minors, the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons".

3 National transposition

This chapter presents relevant developments from different EU countries in the field of national regulation of video-sharing platforms. Its aim is to present, in a non-comprehensive manner, original solutions to some of the most pressing issues in this field.[108] As a basis for this research, we have used, among other sources, our very own IRIS Merlin database,[109] which enables users to access more than 8 000 articles[110] reporting on legal events of relevance to the audiovisual industry.

3.1 General liability regime

As mentioned in Chapter 2 of this publication, a video-sharing platform is not liable for the information stored at the request of a recipient of the service as long as the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent. If the provider obtains such knowledge or awareness, it has to act expeditiously to remove or to disable access to the information (Article 14 ECD). Moreover, providers are not under a general obligation to monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity (Article 15 ECD).

The somewhat "benevolent" liability regime established by the ECD is, in the opinion of some, ripe for reform (see below). Since its adoption in the year 2000, a lot of water has flowed under the bridge. The technical and market developments have been such that the above-mentioned distinction no longer seems adapted to current and future challenges. Hosting providers such as YouTube and Facebook derive direct economic benefit from users' activities. In doing so, they profit massively from all user activities, both legal and illegal, but they wash their hands of their clients' misbehaviour, despite the fact that they utilise algorithms to "steer" the flow of content on their hosted pages.

[108] The European Commission is also currently looking into the matter, see Chapter 6 of this publication.
[109] http://merlin.obs.coe.int/cgi-bin/search.php.
[110] As of March 2018.

3.1.1 France

As an example of the ECD's call for reform, in 2011, a French Senate report[111] proposed to introduce, alongside the hosting provider and the editor of content, a third intermediate category, namely "service editor", whose main characteristic would be to obtain a direct economic benefit from users consulting the hosted content. The "service editor" would have the following obligations:

- identify the persons who have created the content that it hosts;
- put in place the means, in accordance with the state of the art, to monitor the information it transmits or stores and to investigate facts or circumstances revealing unlawful activities. This would be an obligation of means, not of result;
- be held civilly or criminally liable if it becomes aware of manifestly unlawful activities or information and does not act promptly to remove the information or make it impossible to access.

This French report did not have a legislative transposition at national or EU level, but the idea of reforming the status of intermediaries has been on the agenda of the different French governments for many years now. During a speech, the (at the time) French Minister for Culture, Audrey Azoulay, proposed that the platforms also be required to combat the non-respect of human dignity, incitement to racial hatred, and the glorification of terrorism. Thus "we cannot continue to allow the major audiovisual platforms to hide behind a host status that has ceased to correspond to the reality of the services they offer".[112] In a press interview of January 2018, Mounir Mahjoubi, State Secretary for digital issues, insisted on the need for a rethinking of the status of Internet intermediaries.[113]

3.2 Fake news

The development of the so-called "fake news" phenomenon has prompted many countries to propose regulatory action, and in every single case, controversy has followed, with accusations of censorship from different stakeholders. Indeed, the topic has to be handled

[111] Rapport d´information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail sur l'évaluation de la loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon, par MM. Laurent BÉTEILLE et Richard YUNG, Sénateurs. Enregistré à la Présidence du Sénat le 9 février 2011, https://www.senat.fr/rap/r10-296/r10-2961.pdf.

[112] L'audiovisuel dans l'espace numérique : plateformes et données - Actes des Rencontres du CSA du 27 septembre 2016, www.csa.fr/content/download/227230/608057/file/actes%2520rencontres%2520csa_2016.pdf&usg=aovvaw2kstxtlpg0spswghvwii3-.

[113] See, for example, Rees M., "Mounir Mahjoubi : de la loi anti « fake news » à la responsabilité des intermédiaires", Nextinpact, 24 January 2018, https://www.nextinpact.com/news/106025-mounir-mahjoubi-loi-anti-fake-news-a-responsabilite-intermediaires.htm.

with great care: first of all, the status of hosting providers and the prohibition of introducing general monitoring obligations makes it very difficult to regulate this field. Moreover, the contours of the fundamental right to freedom of expression as regulated by Article 10 ECHR leaves the legislator with little room for manoeuvre.

3.2.1 Germany

The *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (Act to improve law enforcement in social networks - NetzDG) was adopted on 1 September 2017 and has spurred a vivid controversy about its chilling effects on freedom of expression online, especially the fact that it leaves too much decisional power to service providers.[114] The first days of its coming into force were particularly controversial as comments from certain politicians were deleted from social media. Germany's opposition parties have called for the abolition of the Act.[115]

The NetzDG applies to telemedia[116] service providers who operate for-profit Internet platforms which are intended for users to share content with other users or to make it accessible to the public (social networks). Platforms with journalistically and editorially designed offers that are the responsibility of the service provider itself are not regarded as social networks within the meaning of this act. The same applies to platforms intended for individual communication or the dissemination of specific content. The obligations included therein only apply to providers whose social networks have more than 2 million registered users in Germany (Article 1(2) NetzDG).

Service providers must ensure, through an effective and transparent procedure, that complaints about unlawful content are immediately noted and checked. Content that is manifestly unlawful must be removed within 24 hours of the complaint being received; all unlawful content must be removed within seven days of the complaint being received; and any decision taken by the provider must be notified to the complainant (Article 3 NetzDG). Unlawful content is defined as content that breaches specific provisions of the *Strafgesetzbuch* (Criminal Code - StGB)[117], such as the rules on slander in Article 185 StGB and certain criminal law provisions on protection from threats to the democratic rule of law (Article 1(3) NetzDG).

---

[114] See, for example, Oltermann Ph., "Tough new German law puts tech firms and free speech in spotlight", The Guardian, 5 January 2018, https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight.

[115] Reuters, "German opposition calls for abolition of online hate speech law", 7 January 2018, https://www.reuters.com/article/us-germany-hatecrime/german-opposition-calls-for-abolition-of-online-hate-speech-law-idUSKBN1EW0Q9.

[116] "Telemedia" are electronic information and communication services which are neither telecommunications services within the meaning of the Telecommunications Act (transmission of signals in telecommunications systems or networks, § 3 Nos. 23 and 24 TKG) are still broadcasting within the meaning of § 2 of the Broadcasting State Treaty (cf. § 1 of the Telemedia Act[TMG] of 26 February 2007[BGBl. I 179] with late amendments). See http://wirtschaftslexikon.gabler.de/Definition/telemedien.html.

[117] Strafgesetzbuch, https://www.gesetze-im-internet.de/stgb/.

The Act requires social network providers to appoint an authorised agent in Germany and to draw attention to this fact on their platform in an easily recognisable and directly accessible manner (Article 5 NetzDG). Providers of social networks that receive more than 100 complaints about illegal content in the calendar year are obliged to prepare a half-yearly report on the handling of complaints about illegal content on their platforms and to publish it in the Federal Gazette and on their own homepage at the latest one month after the end of a six-month period. The report published on one's own homepage must be easily recognisable, immediately accessible and permanently available (Article 2 NetzDG).

3.2.2 France

On 3 January 2018, at his New Year reception for the media, the President of the Republic, Mr Emmanuel Macron, announced that he wanted to change the legal framework which aims to combat "fake news". To this end, a bill has been drafted by the majority group of the French Parliament.

During elections, platforms would be subject to increased transparency obligations on sponsored news content in order to make public the identity of advertisers and those who control them or on whose behalf they act, as well as the amounts devoted to promoting such content.

The draft law also provides for the definition of a duty of cooperation for digital platforms in the fight against the dissemination of false information, with the aim of defining co-regulation mechanisms. This would combine the commitments of digital platforms with supervision by a public authority. At the beginning of 2017, Facebook and Google had simultaneously announced the imminent deployment of arrangements for flagging "fake news" [118] in France: framing the cooperation of platforms should allow these arrangements to be based on criteria that have been the subject of collective and multi-stakeholder discussion.

The proposed law also provides for the creation of a new legal channel to combat misinformation: during electoral periods, it will be possible to bring an action before the judge in summary proceedings, which will enable it to put an urgent stop (within 48 hours) to the dissemination of information that is manifestly false, artificially and massively disseminated, and likely to alter the truthfulness of the ballot.

The draft text also seeks to strengthen the powers of the CSA, the French audiovisual regulator, to combat any attempt at destabilisation or disinformation campaign, carried out by a television service controlled or influenced by a foreign country, through refusal of a convention, suspension of the broadcasting of the service, or termination of its convention, under conditions precisely defined by the text.

[118] See Blocman A., "Facebook and Google join forces with French media to combat fake news", IRIS 2017-3, http://merlin.obs.coe.int/iris/2017/3/article14.en.html.

3.2.3 Italy

Concerning "fake news", a legislative proposal was submitted on 7 February 2017 in the Senate of the Republic.[119] The bill aimed at introducing specific provisions criminalising different conducts relating to the circulation of "fake news". According to the bill:

- Whoever publishes or circulates via the Internet "fake news" or exaggerated or biased information on manifestly ill-founded or false facts and circumstances would be punished by a fine of up to EUR 5 000. In the case of defamation, the aggrieved person could ask for the damages he/she actually suffered and seek additional pecuniary compensation.
- The circulation or communication, including via the Internet, of false, exaggerated or biased rumours or news likely to cause public alarm or threaten public interests in any way, or which may have a misleading impact on the public opinion, would also be punishable by a fine of up to EUR 5 000.
- Whoever carries out, including via the Internet, a hate speech campaign against certain individuals or against the democratic process would be punished by at least two years' imprisonment and a fine of up to EUR 10 000.

The proposal also concerned the ISPs' obligations in respect of the activities and content posted by users. Pursuant to Article 7, ISPs would have to regularly monitor content, paying particular attention to any content that generates a substantial degree of interest among users, in order to assess the reliability and truthfulness of this content. In the event of an ISP determining that certain content does not meet this requirement, it would have to promptly remove the content in question; if the ISP failed to do so, it may be punished in the same way as the actual perpetrator.

After the presentation of the bill, new national elections were called, which implies that this legislative proposal would have to be reintroduced in parliament.

3.2.4 United Kingdom

As part of a wider announcement about a review of its defence capabilities, the UK government announced in January that it would be setting up a dedicated national security unit to tackle "fake news" and disinformation. This unit would be tasked with combatting disinformation "by state actors and others" and would "more systematically deter [the United Kingdom's] adversaries."[120]

---

[119] Senato della Repubblica, disegno di legge n. 2688, 7 febbraio 2017, http://www.senato.it/service/PDF/PDFServer/BGT/01006504.pdf.

[120] Walker P., "New national security unit set up to tackle fake news in UK", The Guardian, 23 January 2018, https://www.theguardian.com/politics/2018/jan/23/new-national-security-unit-will-tackle-spread-of-fake-news-in-uk.

3.3 Protection of minors

The pervasiveness of video-sharing platforms in the lives of children and teenagers is a source of preoccupation for most parents nowadays. They certainly want their children to enjoy all the great things provided by the Internet, but are worried about all the harmful content that is freely available on the very same services. Media literacy is paramount in this regard,[121] and the self-regulation initiatives of the internet industry also play an important role. Nevertheless, the proponents of further regulating the status of internet intermediaries find in the protection of minors a particularly good argument for advancing their proposals, as well as an attentive ear in most parents.

A quite recent example of this tendency for further regulation is the new Internet Safety Strategy[122] announced by UK Culture Secretary Karen Bradley on 11 October 2017.[123] The announced measures propose:

- A new social media code of practice to see a joined-up approach to remove or address bullying, intimidating or humiliating online content;
- An industry-wide levy so that social media companies and communication service providers contribute to raising awareness and countering internet harm;
- An annual internet safety transparency report to show progress on addressing abusive and harmful content and conduct;
- And support for high-tech and digital start-ups to think safety first - ensuring that necessary safety features are built into apps and products from the very start.

The Strategy also outlines the crucial role that education would play in raising online safety awareness, with a particular focus on children and parents:

- New compulsory school subjects – Relationship Education at primary school level and Relationship & Sex Education at secondary school level to provide online safety education;
- Social media safety advice – the government would encourage social media companies to offer safety advice and tools to parents, and safety messages would be built into online platforms;
- Safety features highlighted – the government would work to raise awareness around the safety products and features that are available for parents.

[121] For more information on concrete projects see "Mapping of media literacy practices and actions in EU-28", European Audiovisual Observatory, Strasbourg, 2016, https://rm.coe.int/media-literacy-mapping-report-en-final-pdf/1680783500.

[122] Making Britain the safest place in the world to be online, https://www.gov.uk/government/news/making-britain-the-safest-place-in-the-world-to-be-online.

[123] A consultation on the Internet Safety Strategy green paper ran from 12.15 am on 11 October 2017 to midday on 7 December 2017, https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper.

It is proposed that the UK Council for Child Internet Safety becomes the UK Council for Internet Safety to consider the safety of all users, not just children, and to help deliver the measures within the Strategy.

Concerning online pornography, the Digital Economy Act 2017[124] includes provisions requiring that age verification measures be put in place for commercial pornographic websites. In the absence of such measures, the publisher would become liable to a number of penalties, including fines and Internet service providers being required to block access to their material, including access to any other material the publisher may have. The British Board of Film Classification (BBFC) [125] was designated as the regulator responsible for implementing and enforcing these provisions.[126] The BBFC will be empowered to require information from Internet service provides or any other person it believes to be involved in making pornographic material available on the Internet on a commercial basis. The BBFC will also be able to issue enforcement orders that will be enforceable by the courts in order to prevent the infringement of statutory provisions, and it will have the power to give notice of breaches to payment-services providers so that they can withdraw their services. It will also have the power to require Internet service providers to block access to material, including material other than that which has breached the age verification procedures; such an order would be enforceable by the courts. The only exception to this power is where this would be detrimental to national security or to the prevention or detection of serious crime, including sexual offences.[127]

3.4 Financing content

According to Article 13 of the AVMSD, on-demand audiovisual media services (such as Netflix or Amazon Prime) must abide by a set of obligations in terms of the promotion of European works (for instance, by way of a financial contribution, or the share and/or prominence of European works in their programme catalogues). However, in view of the practice by major pan-European OTT players to choose their country of establishment according to the rules that are more beneficial to them ("jurisdiction shopping"), some

[124] Digital Economy Act 2017, http://www.legislation.gov.uk/ukpga/2017/30/contents/enacted/data.htm.
[125] The Board is responsible for the age classification of films, videos and DVDs, and more recently has been given responsibility for classifying material for mobile network operators to help them in restricting access to materials unsuitable for those under the age of 18.
[126] Department for Digital, Culture, Media & Sport, 'Particulars of Proposed Designation of Age-Verification Regulator, 12 December 2017, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/669567/particulars_of_proposed_designation_of_age-verification_regulator_-_december_2017.pdf.
[127] The minister has issued draft guidance to the regulator on the use of its powers, and guidance will also be issued by the regulator itself. See Guidance from the Secretary of State for Digital, Culture, Media and Sport to the Age-Verification Regulator for Online Pornography, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/673425/Guidance_from_the_Secretary_of_State_for_Digital__Culture__Media_and_Sport_to_the_Age-Verification_Regulator_for_Online_Pornography_-_January_2018.pdf.

countries, like Germany and France, have adopted specific rules aimed at bringing these services under their regulatory framework to create a level playing field with local players, obliging these operators to also contribute to the financial ecosystem of the audiovisual sector.[128] Both schemes have been notified to the European Commission to get the green light from EU competition services.

Video-sharing platforms (like YouTube) are not bound by such obligations at EU level. Indeed, Germany limited the new financial obligation to "holders of licence rights who exploit individual films with a duration of more than 58 minutes in return for payment by means of video-on-demand services".[129] France's new scheme, however, expanded the scope of the national VoD tax not only to foreign VoD services but also to video-sharing platforms; this so-called "YouTube tax", which applies to advertising revenues generated by sites that make free or paid audiovisual content available to the French public,[130] entered into force on 21 September 2017 after having received the Commission's green light.[131] Under the new Article 1609 sexdecies B of the General Tax Code, the tax is due from both the editors of on-demand audiovisual media services and video-sharing platforms (such as YouTube and Dailymotion) if they allow access to audiovisual content. Thus, the tax is payable by any operator, wherever it is established, offering a service in France that gives or permits access, either for free or against payment, to cinematographic or audiovisual works or other audiovisual content. The rate of the tax is to increase from 2% to 10% if the revenue from advertising or sponsorship is connected with "the circulation of cinematographic or audiovisual works of a pornographic or violent nature".

---

[128] For more details on the German and French schemes, see also Cabrera Blázquez F.J., Cappello M., Grece C., Valais S., *VOD, platforms and OTT: which promotion obligations for European works?*, IRIS Plus, European Audiovisual Observatory, Strasbourg, 2016, https://rm.coe.int/1680783489.

[129] Article 66a of the German Film Support Act (FFG) introduces an obligation to contribute to the Federal Film Board to 'video suppliers' and providers of VOD services with a net annual turnover above EUR 50 000. Through an amendment of July 2013, the scope of the film levy was extended to VOD service providers not established in Germany in respect of the income that they derive from selling services on German-language websites to customers in Germany – provided that these transactions are not subject to any comparable financial contribution to the promotion of cinematographic works by a film funding institution in the service's country of origin. The levy is imposed on the service's turnover of video suppliers and VOD providers. Apple and Netflix have challenged the European Commission's decision to approve this legal measure in Germany. See Beschluss der Kommission vom 1.9.2016 über die Beihilferegelung SA.38418 – 2014/C (ex 2014/N), die Deutschland zur Förderung der Filmproduktion und des Filmvertriebs durchzuführen beabsichtigt, http://ec.europa.eu/competition/state_aid/cases/254981/254981_1779719_147_2.pdf.

[130] Décret n° 2017-1364 du 20 septembre 2017 fixant l'entrée en vigueur des dispositions du III de l'article 30 de la loi n° 2013-1279 du 29 décembre 2013 de finances rectificative pour 2013 et des I à III de l'article 56 de la loi n° 2016-1918 du 29 décembre 2016 de finances rectificative pour 2016, https://www.legifrance.gouv.fr/eli/decret/2017/9/20/MICK1721690D/jo/texte/fr.

[131] The European Commission was notified on 3 October 2014 (notification SA.39586 (2014/N). It considered, by decisions of 7 and 8 July 2017, that the notified taxes allocated to the National Centre for Cinema and Movies (CNC) were no longer considered to be an integral part of the various aid measures managed by this establishment and, as such, should no longer be notified when they were extended or amended. No official texts are available at the date of publication of this report. In the German decision, the Commission had acknowledged that the application of the notified tax to services targeted from one member state to the market in another member state shall foresee that the financial contributions be based only on the revenues earned in the targeted member state.

The basis for the so-called "YouTube tax" is the amount of the sums (not including VAT) paid by advertisers and sponsors for the circulation of their advertising and sponsorship messages on the services in question to the taxpayers concerned or to the agencies handing the advertising and sponsorship messages. A flat-rate reduction of 4% is applied to these sums; the reduction is increased to 66% for services giving or allowing access to audiovisual content created by private users for the purpose of sharing and exchange within "communities of interest".

3.5 Protection of copyright

3.5.1 France

In its report on its activities for 2016-2017,[132] the *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet* (high authority for the broadcasting of works and the protection of rights on the Internet - HADOPI) included a number of proposals - some of which would require changes to regulations and legislation - intended to make its actions more effective and adapt them to reflect changes in practices. According to the report, it would be necessary:

- to continue educating the public and to strengthen the awareness programme by tailoring more accurately communication messages to the target public on the gravity of individual behaviour infringing copyright, and by addressing not only the legal issue of the observance of copyright law but all risks faced by Internet users;
- to carry out action jointly with search engines to reduce the visibility of unlawful sites;
- to consider how to improve techniques for detecting sources of piracy;
- to expand, secure and better assess the charter scheme using a "follow the money" approach;
- to ensure a fairer sharing of value by encouraging and accompanying agreements on the introduction of content recognition technologies;
- to define an effective public policy addressing problems arising from the procedures for blocking unlawful sites and their avatars.

In its report, HADOPI proposes several adjustments to regulations and legislation, including simplifying the graduated response procedure; indicating the title of illegally shared works in the recommendations sent to subscription holders; and extending the

[132] HADOPI, Rapport d'activité 2016-2017, https://www.hadopi.fr/sites/default/rapportannuel/HADOPI-Rapport-d-activite-2016-2017.pdf. For more information on copyright enforcement measures see Cabrera Blázquez F.J., Cappello M., Grece C., Valais, S., Copyright enforcement online: policies and mechanisms, IRIS Plus, European Audiovisual Observatory, Strasbourg, 2015, https://rm.coe.int/1680783480.

period during which the public prosecutor may refer cases of copyright infringement to the HADOPI. It also considers it necessary to introduce a public regulation on the use of content recognition technologies. HADOPI would then be able to issue recommendations and, if necessary, act as mediator, observing and assessing ways of implementing agreements between platforms and rightsholders, taking on the role of regulating such agreements, and serving as mediator in the event of disputes. Furthermore, HADOPI should be involved in the fight against sites that infringe copyright on a massive scale. The organisation wants to continue its efforts to combat commercial infringers and is proposing a change in its resources so that it would be able to detect newly emerging unlawful practices at an early stage; investigate the new economic models of unlawful sites; and intervene as a third-party authority to achieve greater involvement on the part of intermediaries.

4 Self-regulation and pan-European initiatives

4.1 The protection of children and young people in video-sharing platforms and social media

Today's children are going online on different devices at an early stage of their lives, sometimes even before being able to read or write. Video-sharing platforms like YouTube have become one of their main sources of entertainment on the Internet. However, according to a 2013 report[133] by the EU Kids Online project,[134] it is also true that children consider video-sharing platforms to be more risky than any other online platform, with pornography and violent content at the top of their list of concerns about web use. There is no doubt that these platforms raise important and challenging issues from the perspective of the protection of minors online. Numerous policies, EU programmes and self-regulatory initiatives have been put in place in Europe over the last few years with a view to empowering and better protecting children and young people (and their parents) online, through the development of skills and tools to use the Internet safely and responsibly.

4.1.1 The approach of video-sharing platforms and social media

In parallel to these pan-European self-regulatory initiatives, social media and video-sharing platforms have also developed their own guidelines and tools to empower users

[133] Livingstone, S., Kirwill, L., Ponte, C., Staksrud, E., "In their own words: What bothers children online?", February 2013, https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf.

[134] EU Kids Online is a multinational research network led in the United Kingdom by the London School of Economics and Political Science (LSE). It seeks to enhance knowledge of European children's online opportunities, risks and safety. It uses multiple methods to map children's and parents' experience of the internet, in dialogue with national and European policy stakeholders. It has been funded by the EC's Better Internet for Kids programme. http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx.

and protect children and young people on their services. The examples of the two most popular video-sharing platforms in Europe – YouTube and Dailymotion – are interesting, as both platforms have chosen slightly different approaches.

4.1.1.1 YouTube

In addition to Google's Community Guidelines,[135] which provide information about the types of content allowed on the company's platforms, YouTube offers a set of security tools to allow users to control their experience and that of their children online. These tools relate either to the users' account or to the content itself.

For example, YouTube uses an age verification system through the Google Accounts unified sign-in system (which also gives users access to products like Gmail). The minimum age requirements vary from 13 to 16 years old, depending on the country. When Google receives a report about an underage account, it is meant to verify the age of the user before disabling the account, asking the user for an identification document. If the account is controlled by an adult, Google requires his/her contact information for verification of consent. Google uses the declared age of the account holder in order to determine whether a user should be shown a video that has been age-restricted.[136] Some videos may also receive an age restriction by Google's review team when they are notified by users or content creators as inappropriate for all audiences. The declared age of the user is also used in order to restrict the exposure of minors to sensitive advertising, including alcohol. YouTube partners are also provided with age-rating tools that they can proactively and voluntarily apply – under their own responsibility – to their paid content, based on different categories of content (strong language, nudity, sexual situations, violence/disturbing material, drug use, and flashing lights).

On the other hand, YouTube users can activate a YouTube Restricted Mode in order to prevent videos with mature content or that have been age-restricted from showing up in a video search, related videos, playlists, shows, or films. This tool is also designed to hide objectionable comments.

Last but not least, in 2015, YouTube developed YouTube Kids, a free standalone app for tablets and mobile phones, targeting exclusively children and family-appropriate entertainment. YouTube Kids comes with different parental control tools, including the ability to remove the search option from the app, giving children access to the pre-selected videos available on the home screen. It also provides a Parental Guide[137] with "important information for grown-ups" in different languages about the functioning of the platform, including the different ways a child can "discover" videos (through searches,

[135] https://support.google.com/youtube/answer/2802032?hl=en.
[136] See more details in "Protection of Minors in the Audiovisual Media Services: Trends & Practices (ERGA report), pp. 54 and following, https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0ahUKEwjOkdeI7t7YAhUFblAKHRRMBZIQFghQMAU&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D44167&usg=AOvVaw3Wwx0pUp6sBIsTTTtuoUQE.
[137] https://support.google.com/youtubekids/?hl=en#topic=6130504.

home screens, recommended videos, a "watch it again" option, etc.). The Guide explains the different parental controls made available (a timer to limit the time spent on the app; blocking content; turning off search options; clearing history; advertising control, etc.). It also gives details about the way the videos available in the app are selected using filters powered by algorithms. However, YouTube also warns users that algorithms are not "perfect", which means that "(…) your child might find content you don't want him or her to watch".

In fact, issues have emerged in the last few years in relation to YouTube search algorithms, both on the main site and in YouTube's stand-alone Kids app, that raise the question of the limits of algorithms and filtering tools for protecting minors: explicit sexual language presented amidst cartoon animation; jokes about paedophilia and drug use; graphic adult discussions about family violence; pornography and child suicide, etc. In these cases, only a posterior control is possible, both through the flagging and reporting of inappropriate content. Under the reporting mechanism set out by Google, anyone who is logged into YouTube and considers that a video (or specific comments) violates the Community Guidelines can flag it and report it by categorising the content violation. The YouTube team then evaluates the content and decides which action to take. It can remove the content globally and immediately in case of clear violation of Google's policy or add an age restriction to the content if this may not be appropriate for all audiences.

In addition, in 2012, YouTube launched the "Trusted Flagger program", in which volunteers (including NGOs and government officials) who have been accepted through an application process are given the authority to flag content that violates the terms of service or Community Guidelines of Google's websites. Google then reviews the flagged content and determines whether to remove it. Pursuing its policy of increasing user empowerment, a few years later, YouTube put in place "YouTube Contributors", a programme designed to recognise and support the global community of people who contribute to the platform by answering questions from YouTube users and producing videos to help users and creators understand how to best use YouTube.

In addition to the Community Guidelines, Google has developed a process to facilitate requests to block content for particular jurisdictions based on local law. Content that violates local law can be reported via Google's legal removals site.[138] Google's team then reviews the material and considers blocking, removing or restricting access to it. Abusive content on Google's services may also violate Google's product policies (which are sometimes more restrictive than the legal norms in certain countries). In these cases, it will be removed from Google's platforms globally. In some cases, content that is allowed under Google's policies may be against the law in a particular country. In these cases, access to such content will be restricted in that country.

Finally, it is worth mentioning that Google has created some Safety Centres and YouTube's Help Centres for specific products, including a comprehensive Parent Resource

[138] https://support.google.com/legal/answer/3110420?hl=en&rd=2.

page that offers tips, advice and further details on safety tools available.[139] In addition, they collaborate with primary schools in several digital awareness-raising programmes to teach children how to stay safe online.

4.1.1.2 Dailymotion

In February 2009, Dailymotion adhered to the European Safer Social Networking Principles[140], as did other companies like Google, Facebook, myspace.com, netlog, bebo, etc. Like YouTube, Dailymotion also provides Community Guidelines that specify how users should behave on the website and the actions they may take should they find inappropriate content. It allows users to set age ratings and restrictions to certain content that may not be seen by all viewers, such as content involving, *inter alia*, violence, nudity and sexually suggestive content, and harmful or dangerous activities. In addition, in 2008, Dailymotion launched DM Kids,[141] an app entirely dedicated to children, which counts on a secure interface, adapted navigation, filtered content, etc.

In terms of reporting, Dailymotion has established a mechanism which allows anyone to flag and notify different types of content classified as harmful (child pornography; dangerous or illegal acts, including but not limited to incitement to violence; animal abuse or drug abuse; unlawful, obscene, defamatory or libellous material; and any sexually explicit content, including but not limited to images of rape, bestiality, intercourse, masturbation, sadistic or masochistic abuse, the explicit depiction of male or female genitalia or pubic areas, paedophilia or necrophilia). Once notified, the Dailymotion team will review the content and possibly remove it from the website. Additionally, the appropriate authorities may be notified. Other tools, such as those used to set age restrictions (based on the level of violence, nudity and sexually suggestive content, and harmful or dangerous activities), are also available. Channels can also use age gates to prevent logged-out users and minors from accessing inappropriate content.

Dailymotion announced in June 2017 a complete redesigning of its app and advertising strategy, with the aim of attracting viewers with higher quality content created through partnerships with media and entertainment brands. However, these changes seems to have impacted more on the solutions offered to protect copyrighted content than in the field of protection of minors, where tools have remained mostly unchanged.[142]

4.1.1.3 Social media platforms: Facebook, Snapchat, etc.

Social media platforms have also taken steps to improve safety and protect minors. For example, Facebook rules state that under -13s cannot sign up (however, research from EU

[139] https://support.google.com/youtube/answer/2802272?hl=en&ref_topic=2803240.
[140] See *op. cit.*
[141] https://www.dailymotion.com/fr/channel/kids/1.
[142] For further details, see at https://www.dailymotion.com/legal/childprotection.

Kids Online and the LSE found that half of 11 to 12-year-olds are on Facebook).[143] Facebook has also entered into partnerships with NGOs to fund counter speech campaigns against bullying, for example. The platform also has "family safety centres" aimed at teens and parents, and encourages users to block or unfriend anyone who is abusive.

Snapchat, another social media platform which is particularly popular among the 11-16 age group (behind Facebook and YouTube), includes in its "Terms of Use"[144] that users must be confirmed to be at least 13 years of age. Snapchat's community guidelines[145] provide that users should not send others material which would constitute harassment or which contains threats or nudity, and, as with other sites and apps, users can block people and report abuses. It also has a safety centre[146] with safety tips and advice, produced in partnership with experts in the field. However, in practice, how many parents really consult these tips…?[147]

4.2 Protection against hate speech and "fake news" in video-sharing platforms and social media

4.2.1 Self-regulatory initiatives against online hate speech

International human rights law requires states to guarantee all people the freedom to seek, receive or impart information or ideas of any kind, regardless of frontiers, through any media of a person's choice, including online platforms. The expression of opinions and ideas is a fundamental human right, protected by Article 19 of the Universal Declaration of Human Rights (UDHR). However, this is not an absolute right and states may, under certain exceptional circumstances, restrict it, notably in respect of the right to equality and the principle of non-discrimination.

In the last few years, a new type of content referred to as "hate speech" has spread online, violating the right to equality and the principle of non-discrimination and obliging us to rethink the right to freedom of expression on the Internet. However, one of the first difficulties when fighting online hate speech relates to the fact that there is no uniform definition of "hate speech" under international human rights law[148] and these variations on

[143] BBC news, *Many under-13s 'using Facebook',* 19 April 2011, http://www.bbc.com/news/technology-13129150.
[144] https://www.snap.com/en-US/terms/.
[145] https://support.snapchat.com/en-GB/a/guidelines.
[146] https://www.snapchat.com/l/en-gb/safety/.
[147] https://familyshare.com/19793/10-things-parents-and-kids-should-know-about-the-snapchat-app.
[148] See Article 19, "'Hate Speech' Explained, A Toolkit", 2015 Edition, p. 3, https://www.article19.org/data/files/medialibrary/38231/'Hate-Speech'-Explained---A-Toolkit-%282015-Edition%29.pdf.

the interpretation of the concept in international instruments are reflected in domestic legislations too.

Back in 1997, the European Court of Human Rights (ECtHR), in a definition adopted by the Council of Europe's Committee of Ministers in the same year, considered "hate speech" as:

> *all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility towards minorities, migrants and people of immigrant origin.*[149]

The UN's International Committee on the Elimination of Racial Discrimination understands "hate speech" as:

> *a form of other-directed speech which rejects the core human rights principles of human dignity and equality and seeks to degrade the standing of individuals and groups in the estimation of society.*[150]

More pragmatically, YouTube, in its Community Guidelines, describes "hate speech" as:

> *(inappropriate) content that promotes or condones violence against individuals or groups based on race or ethnic origin, religion, disability, gender, age, nationality, veteran status, or sexual orientation/gender identity, or whose primary purpose is inciting hatred on the basis of these characteristics.*[151]

On 31 May 2016, the four major platforms (Facebook, Google (YouTube) Twitter and Microsoft), under the aegis of the European Commission, signed a Code of Conduct on countering illegal hate speech online,[152] which included a series of commitments to combat the spreading of such content in Europe. In particular, the platforms pledged to review valid removal notifications against their community guidelines and, where

---

[149] Recommendation No. R(97)20 of the Council of Europe Committee of Ministers on "Hate Speech," 30 October 1997. See also, the European Court of Human Rights (European Court), Gündüz v. Turkey, App. No. 35071/97 (2004), paragraphs 22 and 43. In Recommendation CM/Rec (2010)5 "on measures to combat discrimination on the grounds of sexual orientation or gender identity," the Committee of Ministers has since recommended the following definition for homophobic and transphobic "hate speech": "all forms of expression, including in the media and on the Internet, which may be reasonably understood as likely to produce the effect of inciting, spreading or promoting hatred or other forms of discrimination against lesbian, gay, bisexual and transgender persons", https://rm.coe.int/09000016805cf40a.

[150] UN Committee on the Elimination of Racial Discrimination, General Recommendation No. 35 on combatting racist hate speech, 26 September 2013, CERD/C/GC/35, paragraph 10, http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhssyNNtgI51ma08CMa6o7Bglz8iG4SuOjovEP%2bcqr8joDoVEbW%2bQ1MoWdOTNEV99v6FZp9aSSA1nZya6gtpTo2JUBMI0%2boOmjAwk%2b2xJW%2bC8e.

[151] See *op. cit.*

[152] Code of Conduct on Countering Illegal Hate Speech Online, http://ec.europa.eu/newsroom/document.cfm?doc_id=42985.

necessary, national laws transposing the Framework Decision on combatting racism and xenophobia[153] in less than 24 hours, and to remove or disable access to content, if necessary. The Code also underlined the need to further discuss how to promote transparency and encourage counter and alternative narratives.

According to the third evaluation report of the Code[154], published by the European Commission on 19 January 2018, significant progress has been made by the platforms since the adoption of the Code, as an average of 70% of illegal hate speech notified by NGOs and public bodies has now been removed (compared to 28% in 2016 and 59% in mid-2017). In addition, the report indicates that all participating companies fully meet the target of reviewing the majority of notifications within 24 hours, reaching an average of more than 81% (compared to 51% in mid-2017). The strengthening of the platforms' reporting systems on illegal hate speech is due in part to the platform's staff being better trained and to increased cooperation with civil society, notably through the implementation of the Code and the setting up of a network of "trusted flaggers" throughout Europe.

However, the European Commission considers that further improvements still need to be achieved in relation to transparency and feedback to users, which is still lacking for nearly a third of notifications. In addition, there is still room for improvement in relation to the prosecution of authors of illegal hate speech offenses (online as much as offline). In fact, the Code comes only as a complement to legislations fighting racism and xenophobia which require that authors of illegal hate speech be prosecuted. However, according to the 2018 report, on average, only one in five cases reported to companies were also reported by NGOs to the police and prosecutors.

By focusing on pan-European cooperation to tackle online hate speech, the European Commission has provided a network for cooperation and for the exchange of good practices[155] for national authorities, civil society and companies, as well as targeting financial support and operational guidance. About two thirds of the member states now have in place a national contact point responsible for online hate speech. A dedicated dialogue between competent member state authorities and the platforms is envisaged for the spring of 2018.

4.2.2 Self-regulatory initiatives against "fake news" online

Another phenomenon that raises new challenges for democracy, the rule of law and societies in general relates to the spreading of so-called "fake news" in video-sharing platforms and social media. Although "fake news", also referred to by the Council of

[153] Council Framework Decision 2008/913/JHA of 28 November 2008 on combatting certain forms and expressions of racism and xenophobia by means of criminal law, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Al33178.
[154] http://europa.eu/rapid/press-release_IP-18-261_en.htm.
[155] Countering illegal hate speech online #NoPlace4Hate, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.

Europe in a recent report as "mis-, dis- and mal-information", "information disorder" or "information pollution",[156] has always existed, its impact has been amplified dramatically in a digitally-connected and global world.

The word "post-truth", closely related to the concept of fake news, was actually chosen by the Oxford Dictionaries as Word of the Year in 2016[157] due to the spike in the frequency of its use observed in the context of the EU referendum in the United Kingdom and the presidential election in the United States, respectively in June and November of that same year. The Oxford Dictionaries defines the term as:

> *relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief.*

The impact of "fake news" is still difficult to quantify as we are in the early stages of understanding its implications. While most of the time "fake news" is driven by commercial interest for the sole purpose of attracting visitors from social networks, it may also be driven by partisan or political interests. The role played by video-sharing platforms and social media in relaying fake news like wildfire and causing it to go viral has prompted the major social media companies to assume greater responsibility in the fight against this phenomenon. Self-regulatory initiatives from the industry have multiplied in this field over the last year.

For example, Google first decided to alter its algorithm so that false or offensive information arrives at the tail end of the results when an Internet user carries out a search on a given theme using this engine. It has also asked its team of more than 10 000 people who oversee the research results to report pages that host lies, ill-intentioned hoaxes or conspiracy theories, as well as what the company calls "low-quality" content. Facebook also began experimenting with a system to highlight information from solid journalistic sources on its members' "walls" when confronted with potentially false content. The initiative was called "Related Articles" and was intended to "facilitate access to other perspectives and information", potentially including articles from information verifiers.

However, these tools proved to be inefficient in tackling the spreading of "fake news" on their services and in November 2017, both companies embarked on a second wave of measures. They integrated a new source verification tool into their system which was developed by a consortium of journalists working to develop standards for identifying reliable journalistic production (The Trust Project[158]). This "confidence indicator" takes the form of an icon indicating whether the information source is considered reliable. In concrete terms, this tool takes the form of an icon on which you can click to learn more about the source of the information. Accessible alongside each article shared on Facebook, this icon allows you to know the ethical positioning of the media, as well as

---

[156] See Wardle, C., PhD and Derakhshan, H., "Information disorder: Towards an interdisciplinary framework for research and policy making", Council of Europe report, DGI(2017)09, https://rm.coe.int/information-disorder-report-november-2017/1680764666.

[157] The Oxford Dictionaries Word of the Year is a word or expression that has attracted a great deal of interest over the last 12 months.

[158] https://thetrustproject.org/.

information about how it verifies the information. On 16 November 2017, the consortium announced that Google, Facebook, Bing and Twitter had agreed to use such indicators on their platforms. It remains to be seen whether the integration of this icon on the sites will prove effective. However, social media experts have expressed doubts over the effectiveness of such tools to tackle "fake news" and misinformation on platforms.

Moreover, Facebook, which in 2018 made the fight against "fake news" its main priority, announced in January 2018 a major change in the algorithm of its news feed which will have direct consequences for users and the media. Priority will be given to the content and sharing of users' families and friends. This change in the algorithm is part of an already initiated outlook. Twice already, in April 2015 and June 2016, Facebook gave priority to friends' content in an attempt to relegate the content of the pages to the background. With this latest modification, Facebook wants to return to its original vocation of social networking over passive consumption. As far as users are concerned, the news feed will be more focused on what users want to see, rather than the content that generates the most interaction. This change also means that users will also be more exposed to targeted advertising.[159]

Although the efforts of video-sharing platforms and social media to tackle "fake news" or hate speech have been welcomed, they also raise a number of tricky questions in terms of transparency and accountability. In fact, sites like Facebook, Twitter, Instagram, YouTube and Google+ have an outsized impact on our social lives. We treat these platforms like a "public sphere", using them to discuss both controversial and menial issues, to connect with friends, and to engage in activism and debate. But while these platforms may be used by the public, they are ultimately owned by private companies with their own rules and systems of governance that control—and in some cases, can censor—users' content. The dilemma for these platforms is to know where the fight against misinformation ends and the practice of censorship starts. Some initiatives have popped up in this field, such as the platform Onlinecensorship.org[160], which seeks to encourage companies to operate with greater transparency and accountability towards their users, since they make decisions that regulate speech. The question of which role the legislator should play in this field has also been raised.

4.3 The protection of copyright-protected content in video-sharing platforms and social media

As previously explained, under the E-commerce Directive, Internet service providers should not be held liable for the content they transmit, store or host, as long as they act in a strictly passive manner. Article 14 of the ECD states that they cannot be held liable for illegal content provided that they do not have knowledge of an illegal activity or that

[159] https://www.ouest-france.fr/high-tech/facebook/facebook-fait-appel-ses-utilisateurs-pour-lutter-contre-les-fake-news-5512942.

[160] See for example "online censorship", https://onlinecensorship.org/about/what-we-do.

they act expeditiously to remove it or disable access to it as soon as they become aware of it.[161] Moreover, the ECD encourages the drawing up of codes of conduct at EU level and voluntary agreements within the industry, as well as so-called "Notice and action" procedures for illegal content.[162]

The industry has been very active in setting up voluntary procedures for the handling of requests to remove illegal content on the Internet. Under notice and action (also referred to as "Notice and Take-down" – NTD)[163] procedures, stakeholders can notify the platform of illegal content on their website and the platform must take it down as soon as possible.[164] NTD procedures are frequently invoked to remove copyright-protected content in video-sharing platforms, considering the role such platforms play in the distribution of audiovisual content.[165]

For example, YouTube's Content ID,[166] which is closely related to NTD procedures based on the DMCA, provides rightsholders with an automated, scalable system enabling them to identify YouTube videos that include content they own. Content ID can be used by rightsholders who own exclusive rights to a substantial body of original material that is frequently uploaded by the YouTube user community. Rightsholders provide YouTube with reference files (audio, visual, or audiovisual) and metadata that describe the content and which territories they own it in. These files are then used by YouTube to scan uploaded videos for matching content. When a match is found, YouTube applies the rightsholders preferred policy: to monetise, track, or block the video in question. Content ID also performs a "legacy scan" to identify matching videos uploaded before the reference. A full legacy scan may take a number of months to complete; recent uploads and popular videos are scanned first.

It is also worth mentioning the collaboration of video-sharing platforms with collective rights management organisations concerning the distribution of the works of their members on video-sharing platforms. For example, in France, YouTube has recently renewed its agreement with the SACD (Society of Dramatic Authors and Composers) and ADAGP (Society of Authors in Graphic and Plastic Arts). As a result of this collaboration

---

[161] For further details, see Cabrera Blázquez F., Cappello M., Grece C., Valais, S., *Copyright enforcement online: policies and mechanisms*, IRIS Plus, European Audiovisual Observatory, Strasbourg, 2015, p. https://rm.coe.int/1680783480.

[162] Illegal content includes a wide range of issues, including infringement of intellectual property rights (trademark or copyright), child pornography, racist and xenophobic content, defamation, terrorism or violence, illegal gambling, illegal pharmaceutical offers, illicit tobacco or alcohol advertisement, etc.

[163] According to the US Digital Millenium Copyright Act (DMCA), the expeditious removal (the "Takedown") of content protected by copyright upon receipt of a notification (the "Notice") exempts the intermediary from any liability with regard to the copyright violation. This procedure is employed by all US-based websites and is considered to be a quick and economical remedy against copyright violations.

[164] Blocking may become the only solution when takedown is not possible because the illegal content is stored in a different country from the one where the servers of the platform are located.

[165] For further details, see IRIS Plus on *Copyright enforcement online: policies and mechanisms, op. cit.*, p. 52 and following.

[166] See YouTube "Using Content ID", https://support.google.com/youtube/answer/3244015?hl=en&ref_topic=4515467&vid=1-635799113680735986-2037337187.

launched in 2010, the authors represented by both societies will continue to receive, via the societies of authors of which they are members, royalties corresponding to the exploitation of their works by content creators and suppliers on YouTube.[167]

As for Dailymotion, in the last few years, the platform has carried out a reshifting in its activities, moving away from predominantly user-generated content (UGC) and towards more premium publisher partnerships and exclusive content.[168] This strategy shift has been accompanied by an optimisation of the protection of copyrighted content, through copyright notifications procedures and content filtering solutions. Users who believe that their works have been copied illegally can file a claim for copyright infringement to Dailymotion's copyright agent on its site, providing detailed information on the ownership of rights, the work in question, its location on the Internet, etc.[169]

In addition, Dailymotion has strengthened its collaboration with rightsholders to work on innovative content protection systems based on audio and video fingerprinting, developed by Audible Magic and the Institut National de l'Audiovisuel (National Institute for the Audiovisual, INA). According to this system, content owners can provide these companies with the digital fingerprint of their content. All videos posted on Dailymotion are compared to the INA and Audible Magic audio and video fingerprint databases and each time the platform identifies a video that matches a fingerprint, it blocks its distribution before it is published on the site.[170]

As for Facebook, the social media platform also provides for a takedown notice procedure based on the DMCA. However, the procedure for reporting copyright infringement seems to be less intuitive and straightforward than the user interface itself, as it includes numerous steps, from locating the form on the website, to answering preliminary questions, before identifying the content and the rightsholder themselves.[171]

4.4 The limits of targeted advertising on online platforms

EU law encourages self- and co-regulation in the advertising sector, seen as offering efficient approaches, providing higher chances of industry accountability, faster-paced decision-making and greater sustainability. Accordingly, many self- and co-regulatory mechanisms are in place at international, EU and national levels in relation to commercial communications, including in the online environment.[172] Of particular relevance for video-

[167] See for example in France, *YouTube, la SACD, et l'ADAGP renouvellent leur accord,* 11 January 2018, https://www.sacd.fr/youtube-la-sacd-et-ladagp-renouvellent-leur-accord-0 and *YouTube, the SACD and the ADAGP renew their agreement,* https://www.adagp.fr/en/actuality/youtube-sacd-and-adagp-renew-their-agreement.

[168] https://venturebeat.com/2017/06/21/dailymotion-reboots-itself-with-new-premium-video-service/.

[169] https://www.dailymotion.com/legal/copyright.

[170] https://www.dailymotion.com/legal/contentprotection.

[171] https://www.facebook.com/help/contact/937027619679465.

[172] For further details, see Cabrera Blázquez F.J., Cappello M., Grece C., Valais S., *Commercial communications in the AVMSD revision*, IRIS Plus, European Audiovisual Observatory, Strasbourg, 2017, p. 39 and following,

sharing platforms and social media (and more generally for online platforms) is a new type of personalised and targeted advertising based on the monitoring of people's online behaviour, which is referred to as "online behavioural advertising" (OBA). OBA exploits users' data collected through tracking cookies and other technologies, such as flash cookies and device fingerprints. These cookies allow companies to collect detailed information on users based on their web browsing data, search histories, media consumption data (such as videos watched), app use data, purchases, click-through responses to ads, and communication content, such as what people write in e-mails (for example via Gmail) or post on social networking sites.[173] Contrary to other types of online advertising, OBA uses personal information to tailor advertisements in such a way that they are perceived as more personally relevant.

This practice may be particularly beneficial to advertisers, but it also raises serious concerns about privacy and transparency for users. For example, the tracking of online activities and the collection of behavioural data often happen while users are unaware of it. Despite the fact that companies are required under privacy laws to comply with certain transparency obligations related to their data processing practices, for example through privacy statements on their platforms, users seldom read such statements and tend to agree with almost all requests, or simply ignore them.[174]

The online advertising industry has developed self-regulatory approaches to improve transparency that entail the explicit disclosure of data collection, usage, and distribution. At international level, the International Chamber of Commerce (ICC) has addressed the concerns raised by OBA in the "Consolidated Code of Advertising and Marketing Practice",[175] with an updated section dealing with issues specific to digital interactive media techniques and platforms. The ICC defines OBA as:

> *the practice of collecting information about a user's online activity over time, on a particular device and across different, unrelated websites, in order to deliver advertisements tailored to that user's interests and preferences.*

The ICC Code of self-regulation on the use of digital interactive media provides a series of recommendations, guidance and standards to companies engaged in OBA with a view to protecting users.[176]

Numerous self-regulatory organisations (SROs) are also active in the field of online advertising in Europe. Their objective is to provide a complete and integrated pan-

---

http://www.obs.coe.int/documents/205595/8682894/IRIS+Plus+2017-2+Commercial+communications+in+the+AVMSD+revision/783f02df-ff10-447c-a144-43b70b19b218.

[173] Zuiderveen Borgesius, Frederik J. (2015a), *Improving Privacy Protection in the Area of Behavioural Targeting*, Alphen aan de Rijn, the Netherlands: Kluwer Law International.

[174] Boerman, S., C., Kruikemeier, S., Zuiderveens Borgesius, F., J., *Online Behavioral Advertising: A Literature Review and Research Agenda*, http://www.tandfonline.com/doi/full/10.1080/00913367.2017.1339368.

[175] Consolidated ICC Code, available at: https://iccwbo.org/publication/advertising-and-marketing-communication-practice-consolidated-icc-code/.

[176] See more details at https://iccwbo.org/global-issues-trends/responsible-business/marketing-advertising/digital-marketing-communication/.

European industry-wide approach for OBA based on self-regulatory solutions, and to implement a coherent minimum harmonised approach across the EU/EEA. They develop standards, guidance and codes of conduct for the industry in relation to OBA, which may in some cases be binding upon their members.

Among the principles put forward by SROs, the need for transparency for users comes out top. In practical terms, it usually means that companies engaged in OBA should provide a privacy notice on their website about data collection and use practices.[177] In addition, explicit consent from users should be obtained on a prior basis by companies that use specific technologies or practices, such as browser toolbars, to collect data about all or substantially all websites that are visited on a particular computer or device and that use such data for delivering OBA. Furthermore, companies should provide clear and transparent mechanisms to enable consumers to choose not to have their data collected for advertising or marketing purposes.[178] In addition, "sensitive" segmentation based on categories of interest is usually recommended, for example to impede the specific targeting of children, or in relation to sensitive personal data, where the web user's prior explicit content should be obtained. Finally, effective mechanisms to ensure compliance with and the handling of complaints concerning standards should be put in place.

It is also worthwhile noting the efforts of video-sharing platforms to improve their transparency standards in advertising. Thus, for example, on 17 November 2017, the Dutch Media Authority (*Commissariaat voor de Media*) announced a self-regulatory code on transparency in YouTube advertising, the *Social Code: YouTube, in order to be more transparent about advertising in online videos*.[179] The code was developed by a large group of YouTube users who create professional online video content with the help of the Dutch Media Authority, in response to the results of research by the Dutch Media Authority on the frequency with which products and brands are visually shown in videos on YouTube. During the development of this Code, several parties, including the Dutch Advertising Code Authority (*Stichting Reclame Code*), Multi-Channel Networks (third-party service providers for YouTube channels), media agencies and interest groups were given the opportunity to submit views. The Code was also informed by a study on how to enhance transparency in advertising, commissioned by the Dutch Media Authority. In this Code, YouTube video creators have established guidelines about how to indicate advertisements in their videos (for example, when they are paid to promote a particular product or brand). The Code attempts to create clarity for online creators of videos, but also for viewers, parents of underage viewers, companies representing YouTube users and advertisers. A first evaluation of the Code by the Dutch Media Authority is planned for the Spring of 2018.[180]

---

[177] An enhanced notice to inform consumers whenever they are collecting or using data for OBA purposes on a website that is not operated by them is also sometimes recommended.

[178] This is usually done in the form of an icon linking to an OBA "user choice sites".

[179] https://www.desocialcode.nl/.

[180] For more details, see Hanhart, M.J.A., Institute for Information Law (IViR), University of Amsterdam, IRIS newsletter 2018/2, https://merlin.obs.coe.int/iris/2018/2/article27.en.html.

The following table includes some of the main SROs in Europe that are active in the field of OBA.

Table 1. Online Advertising Self-Regulatory Organisations

Organisations	Mandate	Codes / Guidelines / Tools
Interactive Advertising Bureau (IAB)	Member organisation for media and marketing industries active in the digital economy. Its members are responsible for buying, selling, optimising, and analysing digital advertising and marketing campaigns. Develops technical standards, best practices, and research, with emphasis on education and awareness raising among brands, agencies, and the general business community regarding the value of digital advertising.	*IAB Europe's Online Behavioural Advertising (OBA) Framework*: Structure for codifying industry good practices and principles to increase transparency and choice for web users within the EU/EEA, which are binding upon members (for example, ad reporting, control, icon, explicit consent, OBA user choice site, etc.). *Your Online Choice*: Consumer-focused website and education portal in all EU languages, providing a mechanism for web users to exercise their choice with respect to the collection and use of data for OBA purposes.
European Advertising Standards Alliance (EASA)	The EASA brings together 34 national advertising SROs and 16 organisations representing the advertising industry (including IAB Europe) in Europe and beyond to promote high ethical standards in commercial communications, through EASA's Advertising Self-Regulatory Charter and EASA's Best Practices Recommendations.	*EASA's Best Practices Recommendations on OBA*: (adopted on 7 April 2011 and implemented by national SROs in Europe and EASA industry members). Sets out a European advertising industry-wide self-regulatory standard and a compliance mechanism for consumer controls in OBA.
European Interactive Digital Advertising Alliance (EDAA)	Leading alliance of digital advertising organisations in the EU, with the goal of introducing EU-wide standards to "enhance transparency and user control for online behavioural advertising".	Bases its objectives on IAB Europe's Online Behavioural Advertising (OBA) Framework and the European Advertising Standards Alliance's Best Practices for online behavioural advertising.
Network Advertising Initiative (NAI)	Non-profit SRO focused on responsible data collection and use in online advertising, with emphasis on third-party advertising technology companies	*Code of conduct* (last updated in 2018): Assesses the types of data that member companies can use for advertising purposes, and imposes restrictions on the member companies' collection, use, and transfer of data used for personalised advertising; *Consumer Opt-out page*:

		Website where Internet users can opt out of receiving online advertising from NAI members who use HTTP cookies on computer browsers.
Digital Advertising Alliance (DAA)	Online advertising industry association made up of other member organisations, focusing on ethical self-regulation in the online advertising and ad tech industries, whose purpose is to expand self-regulation for interest-based advertising to the entire ecosystem.	*Advertising Option Icon ("Ad Choices" icon)*, which publishers can place on their pages offering users options about what happens when they encounter advertising on their page and how they interact with that advertising; Provides a self-regulatory programme, recommendations, and misconduct reporting resources for Internet users and companies involved with digital advertising.
Trustworthy Accountability Group (TAG)	Cross-industry collaboration to foster transparency in digital advertising business relationships and transactions.	Focus on eliminating fraudulent digital advertising traffic, combatting malware, fighting ad-supported Internet piracy to promote brand integrity, and promoting brand safety through greater transparency.
Direct Marketing Association (DMA)	Global member organisation whose mission is to advance and protect responsible data-driven marketing, both on- and offline.	Advocates policy that promotes the use of ethical data-driven marketing with positive outcomes for both end-users and marketers. Hosts the Dynamic State of Data conference "to discuss issues affecting data-driving marketers with leading policymakers of the day".

5 Case law

5.1 The European Court of Human Rights

5.1.1 Freedom of expression v. hate speech in video-sharing platforms and social media

The right to freedom of expression is protected under Article 10, paragraph 1 of the European Convention on Human Rights (ECHR). This right is one of the essential pillars of a democratic and pluralistic society and it includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. According to the European Court of Human Rights' (ECtHR) caselaw, the right to freedom of expression:

> *(...) is applicable not only "to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population."* (case *Handyside v. the United Kingdom*)[181]

However, as a limit to this right, the Court has also clarified that

> *(...) as a matter of principle it may be considered necessary in certain democratic societies to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance ..., provided that any 'formalities', 'conditions', 'restrictions' or 'penalties' imposed are proportionate to the legitimate aim pursued."* (case *Erbakan v. Turkey*).[182]

Based on these principles, the ECtHR's approach to incitement to hatred and freedom of expression online is twofold:

[181] Judgment of the ECtHR of 7 December 1976, case *Handyside v. the United Kingdom*, (Application no. 5493/72*)* § 49, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57499%22]}.
[182] Judgment of the ECtHR of 6 July 2006, case *Erbakan v. Turkey*, (Application no. 59405/00) § 56, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-76232%22]}.

- First, the exclusion from the protection of the Convention (based on Article 17 on the prohibition of abuse of rights)[183], where the comments in question amount to hate speech and negate the fundamental value of the Convention,[184] and
- Secondly, the setting of restrictions to the right to freedom of expression (based on Article 10, paragraph 2 of the Convention,[185] where the speech in question, although it is hate speech, is not apt to destroy the fundamental values of the Convention).

Video-sharing platforms and social media, like any other online platforms providing user-generated content, assume the "duties and responsibilities" associated with freedom of expression in accordance with Article 10 § 2 of the Convention, where users disseminate hate speech or comments amounting to direct incitement to violence. Although the ECtHR has dealt extensively in its caselaw with hate speech, including ethnic hate, negationism and revisionism, racial hate, religious hate, and threat to the democratic order,[186] only a few cases related specifically to hate speech in online platforms, as presented below.

5.1.1.1 Hate speech and the negation of the fundamental values of the European Convention on Human Rights

The ECtHR had to pronounce itself in the *Belkacem v. Belgium* case[187] on the fine line between freedom of expression and hate speech in video-sharing platforms. The case concerned the conviction of Mr Belkacem, the leader and spokesperson of the organisation "Sharia4Belgium", which was dissolved in 2012 for incitement to discrimination, hatred and violence on account of remarks he made in YouTube videos concerning non-Muslim groups and Sharia law. Relying on Article 10 of the ECHR, Mr Belkacem argued before the ECtHR that he had never intended to incite others to hatred, violence or discrimination but had simply sought to propagate his ideas and opinions. He maintained that his remarks had merely been a manifestation of his freedom of expression and religion and had not constituted a threat to public order.

---

[183] This provision is aimed at preventing persons from inferring from the Convention any right to engage in activities or perform acts aimed at the destruction of any of the rights and freedoms set forth in the Convention.

[184] See ECtHR (Second Section), Decision as to the admissibility of 18 May 2004, case *Seurot v. France*, (Application No. 57383/00), https://hudoc.echr.coe.int/eng#{"itemid":["001-45005"]}.

[185] Article 10 § 2 of the ECHR provides as follows: "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restriction or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of other, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

[186] For more details, see also ECtHR, Factsheet – Hate speech, July 2017, http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf.

[187] ECtHR (Second Section) Decision of 27 June 2017, case *Belkacem v. Belgium,* (Application No. 34367/14) , https://hudoc.echr.coe.int/eng#{"itemid":["001-175941"]}.

The Court considered that the remarks in question had markedly hateful content and that Mr Belkacem, through his recordings, had sought to stir up hatred, discrimination and violence towards all non-Muslims. In the Court's view, such a general and vehement attack was incompatible with the values of tolerance, social peace and non-discrimination underlying the European Convention. The Court therefore rejected the application, finding that it was incompatible with the provisions of the Convention and that Mr Belkacem had attempted to deflect Article 10 of the Convention from its real purpose by using his right to freedom of expression for ends which were manifestly contrary to the spirit of the Convention.

5.1.1.2 The liability of Internet news portals for hate (and offensive) speech posted by users

5.1.1.2.1 The limits to the liability exemption for extreme comments posted by users on a commercially-run Internet news portal

The case *Delfi AS v. Estonia*[188] was the first case in which the ECtHR had been called upon to examine, from the perspective of the right to freedom of expression, a complaint about the liability for user-generated comments (UGC) on an Internet news portal. The applicant company, Delfi AS, which runs a news portal on a commercial basis, complained that it had been held liable by the national Estonian courts for the offensive comments posted by its readers below one of its online news articles about a ferry company. At the request of the lawyers of the owner of the ferry company, Delfi removed the offensive comments about six weeks after their publication.

The case thus concerned the duties and responsibilities of an Internet news portal which provided on a commercial basis a platform for UGC on previously published content, and some users – whether identified or anonymous – engaged in clearly unlawful hate speech which infringed the personality rights of others. The Delfi case did not concern other fora on the Internet where third-party comments can be disseminated, such as Internet discussion fora or social media platforms. Moreover, the question before the Grand Chamber was whether holding Delfi liable for comments posted by third parties had been in breach of its freedom to impart information (and not about the freedom of expression of the authors of the comments).

The Grand Chamber found that the national courts' finding of liability against Delfi had been a justified and proportionate restriction on the portal's freedom of expression, for the following main reasons, and that it shall not be understood as imposing a form of "private censorship"[189]:

---

[188] Judgment of the ECtHR (Grand Chamber) of 16 June 2015, case *Delfi AS v. Estonia*, (Application no. 64569/09), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22003-5110487-6300958%22]}.

[189] See also Voorhoof D., *Delfi AS v. Estonia* (Grand Chamber), IRIS 2015-7/1, European Audiovisual Observatory, Strasbourg, France, http://merlin.obs.coe.int/iris/2015/7/article1.en.html.

- First, because the comments in question had been extreme and had been posted in reaction to an article published by Delfi on its professionally managed news portal run on a commercial basis. In this case, the Court considered that the liability exemption did not apply to Delfi, as its involvement in making public the comments on its news articles on its news portal go beyond that of a passive, purely technical service provider and that it had exercised a substantial degree of control over the comments published on its portal.190
- Secondly, because the steps taken by Delfi to remove the offensive comments without delay after their publication had been insufficient. The Grand Chamber also made clear that the establishment of the unlawful nature of the disputed comments did not require any linguistic or legal analysis by Delfi, since it was plain to see that the remarks were manifestly unlawful.

5.1.1.2.2 Non-liability for offensive comments posted by users on a for non-profit news portal

Contrary to the Delfi case, on 2 February 2016, the ECtHR held in the *Magyar Tartalomszolgáltatók Egyesülete and Indew.hu* case[191] that a self-regulatory body of Internet content providers and an Internet news portal were not liable for vulgar and offensive online comments posted on their websites. The case concerned the complaint by a self-regulatory body (Magyar Tartalomszolgáltatók Egyesülete) and a news portal (Index.hu Zrt) that they had been held liable by the national courts for online comments posted by their readers following the publication of an opinion criticising the misleading business practices of two real estate websites.

The ECtHR reiterated that, although they were not publishers of comments in the traditional sense, Internet news portals had, in principle, to assume duties and responsibilities. However, the Court considered that the Hungarian courts, when deciding on the notion of liability in the applicants' case, had not carried out a proper balancing exercise between the competing rights involved, namely between the applicants' right to freedom of expression and the real estate websites' right to respect for its commercial reputation.

It is to be noted that the applicants' case was, in some respects, different from the *Delfi AS v. Estonia case* as it was notably devoid of the pivotal elements in the *Delfi AS* case of hate speech and incitement to violence. Although offensive and vulgar, the comments

[190] The reason why Delfi could not rely on the limited liability regime for Internet service providers (ISPs) of Article 12 to 15 of the Directive 2001/31/EC on Electronic Commerce was, according to the Estonian courts, that the news portal had integrated the readers' comments into its news portal, it had some control over the incoming or posted comments and it had invited the users to post comments, while it also had an economic interest in exploiting its news platform through the integrated comment environment. The ECtHR did not challenge this finding by the Estonian courts, restricting its supervisory role to ascertaining whether the effects of refusing to treat Delfi as an ISP were compatible with Article 10 of the Convention.

[191] Judgment of the ECtHR (Chamber) of 2 February 2016, case *Magyar Tartalomszolgáltatók Egyesülete* and *Index.hu Zrt v. Hungary*, (Application No. 22947/13), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160314%22]}.

in the present case had not constituted clearly unlawful speech. Furthermore, while Index is the owner of a large media outlet which must be regarded as having economic interests, MTE is a non-profit self-regulatory association of Internet service providers, with no such known interests.[192]

5.1.1.2.3 Freedom of expression and dissemination of false information

Concerning the issue of "fake news" in video-sharing platforms, the ECtHR has not been required to address this issue thus far. However, in a judgment of 2005, it shed an interesting light on the scope of the notion of "dissemination of false information" in light of the freedom of expression in the case *Salov v. Ukraine*.[193] In particular, the Court confirmed that:

> *"(…) Article 10 of the Convention as such does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful. To suggest otherwise would deprive persons of the right to express their views and opinions about statements made in the mass media and would thus place an unreasonable restriction on the freedom of expression set forth in Article 10 of the Convention."* (§ 113)

5.2 The Court of Justice of the European Union

5.2.1 The definition of video-sharing platforms

In a recent case referred to the Court of Justice of the European Union (CJEU) by the Bundesgerichtshof (German Federal Supreme Court), the national Court had to pronounce itself on the question of the qualification of a YouTube video channel with short advertising videos in relation to the definitions provided in the AVMSD.

The case concerned a short video posted on a video channel run by Peugeot Deutschland on YouTube about a new Peugeot vehicle. Deutsche Umwelthilfe[194] brought an action against Peugeot Deutschland before the Landgericht Köln (Regional Court, Cologne, Germany) claiming that the failure to provide, in that video, information on the

---

[192] See also on the same topic: ECtHR Decision as to the admissibility of 7 February 2017, case *Pihl v. Sweden* (Application No. 74742/14), https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-172145%22]}. See also, Voorhoof D., *Rolf Anders Daniel Pihl v. Sweden*, IRIS 2017-9/1, European Audiovisual Observatory, Strasbourg, France, http://merlin.obs.coe.int/iris/2017/5/article3.en.html.

[193] Judgment of the ECtHR, *Salov. V. Ukraine*, Application No. 65518/01, 6 September 2005, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-70096%22]}.

[194] Deutsche Umwelthilfe is a non-profit environmental and consumer protection association, supported by public and private project grants and donations. It is a member of the European Environmental Bureau, in Brussels.

official fuel consumption and official specific CO_2 emissions of the new vehicle model being advertised infringed German regulation on consumer information on fuel consumption, CO_2 emissions and energy consumption of new passenger cars ('the Pkw-ENVKV'). The question of whether the provision of a promotional video channel on YouTube constitutes an "audiovisual media service" within the meaning of Article 1(1)(a) of the AVMSD was referred to the CJEU.

By judgment of 21 February 2018,[195] the Court found that a promotional video channel on YouTube cannot be regarded as having as its principal purpose the provision of programmes in order to inform, entertain or educate the general public. The purpose of such a video is to promote, for purely commercial purposes, the product or service advertised. Even in the event that it would display the features of an audiovisual media service, its promotional purpose suffices to exclude it from the scope of Article 1(1)(a) of the AVMSD. In addition, the Court distinguishes these videos from "audiovisual commercial communications" under the meaning of the AVMSD, as they cannot be regarded as accompanying or being included in a programme in return for payment or for similar consideration or for self-promotional purposes. The Court concludes that the definition of AVMS "*covers neither a video channel, (…) on which Internet users can view short promotional videos for new passenger car models, nor a single video of that kind considered in isolation.*"

5.2.2 Online platforms and copyright infringement

5.2.2.1 The notion of "active" or "passive" hosting providers

As new kinds of "hosting" providers have emerged that were not envisaged at the time of adoption of the E-Commerce Directive (ECD), the CJEU has been referred to on many occasions concerning the qualification as "hosting services" of certain online platforms and the ability of such platforms to benefit from the liability exemption regime set out by Article 14(1) of the ECD.

The CJEU understood Article 14 of the ECD as applying only to providing services neutrally by a merely technical and automatic processing of data provided to its customers. In other words, the criteria used by the Court has been to consider the "active" or "passive" role of the platforms over the information they store. An active role may, for example, refer to activities such as indexing, suggesting and branding the information stored. An active or passive role is assessed by the Court on a case-by-case basis.[196]

---

[195] Case C-132/17, *Peugeot Deutschland GmbH v Deutsche Umwelthilfe eV,* 21 February 2018, http://curia.europa.eu/juris/document/document.jsf?text=&docid=199509&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=554872.

[196] See also Cabrera Blázquez F.J., Cappello M., Grece C., Valais, S., *Copyright enforcement online: policies and mechanisms*, IRIS Plus, European Audiovisual Observatory, Strasbourg, 2015, p. 62 and following, https://rm.coe.int/1680783480.

Table 2. Selected EU caselaw concerning the notion of "hosting" provider

Case reference	Key issue	CJEU's decision
Joined Cases C-236/08 to C-238/08 *Louis Vuitton v. Google*	Louis Vuitton and other trademark owners sued Google for trademark infringement in relation to Google online advertising service "AdWords" (where advertisers pay Google based on the frequency with which users click on their advertisement). The CJEU had to determine whether AdWords should be classed as an Internet "hosting" service provider (benefitting from the liability exemption of Article 14 ECD) or an Internet content provider.	AdWords is an information society service. However, Google can benefit from the liability exemption regime only if it proves that its role is "…neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores." The key element to determining the extent to which the exemption of liability applies to an online platform depends on whether the platform has active control over and knowledge of the information stored or transmitted.
C-324/09 *L'Oreal v. eBay*	L'Oréal sued eBay for being allegedly involved in trademark infringements committed by users of its website. The CJEU was referred to for a preliminary ruling on the interpretation of Article 14 ECD. The assistance provided by the platform to its users, for example optimising the advertisement of their offers, is an indicator of the "active role" of the platform.	Article 14 ECD "…must be interpreted as applying to the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored." The same conclusion applied here as to the "active role" played by the online platform (hosting service provider) related to its knowledge and/or control over the information stored or transmitted.
C-434/15 *Associacion Profesional Elite Taxi v. Uber Systems Spain S.L.*	The electronic platform Uber provides, by means of a smartphone application, a paid service consisting of connecting non-professional drivers using their own vehicles with persons who wish to make urban journeys. The CJEU had to give a preliminary ruling on the extent to which UberPop can operate in Spain without an authorisation from the competent Spanish authorities. The Court had to clarify whether UberPop is a transport service provider or an information society service within the meaning of the ECD.	The Court took the view that the service provided by Uber is more than an intermediary service. The Court notes that the application provided by Uber is indispensable for both the drivers and the persons who wish to make an urban journey. It also points out that Uber exercises decisive influence over the conditions under which the drivers provide their service. Therefore, it must be regarded as forming an integral part of an overall service whose main component is a transport service and, accordingly, must be classified not as an "information society service" but as "a service in the field of transport". This case is interesting, as it shows how determining the nature of parties to transactions (that is to say, traders or consumers) is essential to identifying the applicable legislation.

5.2.2.2 The liability exemption privilege of hosting and access providers

Article 14(1) a) of the ECD only includes into the liability exemption privilege information society services which do not have actual knowledge of illegal activity or information and,

as regards claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent. Article 14(1) b) of the ECD further requires that the information society service, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

The CJEU has not yet decided upon the criterion of knowledge within Article 14 of the ECD. However, the Court interprets Article 14(1) a) and b) of the ECD in such a way that a hosting provider loses its privilege and in particular is liable for damages if it does not act as a "*diligent economic operator*". The hosting provider is thus denied the privilege in cases where it had been aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question and did not act expeditiously in accordance with Article 14(1) b) of the Directive.[197]

The criteria of "actual knowledge" of the specific infringement committed may seem too narrow though to address the massive infringement of copyright-protected content on certain video-sharing platforms, such as p2p platforms, whose business model is based on enabling users to download and share attractive files on a premium account against remuneration.

Another type of information society services which are granted a liability privilege under Article 12 of the ECD is access providers, as long as they are neutral "mere conduit" providers. However, here too, new access provider business models have emerged since the Directive was adopted which are on the borderline between access providers and hosting providers and which play an important role in disseminating live streams for certain customers (for example, the dissemination of football matches by upstream providers to larger audiences, infringing copyright exclusive licensing to pay-TV channels).[198]

5.2.2.3 Link providers

Linking is one of the key aspects of the Internet, and numerous online platforms are dedicated to producing, collecting and indexing links, starting with services such as search engines or video-sharing platforms, which provide links to Internet users to help them find content. Despite the considerable importance of linking providers on the Internet, the application of the liability privilege of Articles 12 to 14 of the ECD is, to a certain extent, still unclear.

The CJEU has clarified that "referencing service providers" fall within Article 14 of the Directive for their paid-for links, that is to say, links advertising third-party products and services.[199] In addition, the Court has developed its own liability rules for linking

[197] CJEU case C-324/09, *L'Oréal v. eBay*, 12 July 2011, paragraph 120 et seq., http://curia.europa.eu/juris/document/document.jsf?text=&docid=107261&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=687263.

[198] For further details, see "Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?", Directorate-General for Internal Policies, 2018, p 14, http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA(2017)614207_EN.pdf.

[199] CJEU joined cases C-236/08 to C-238/08, Google and Google France, 23 March 2010, para. 110,

providers through its case law in *Svensson and Others, GS Media/Sanoma*, *Stichting Brein* and *Ziggo/Brein ("the PirateBay")* (see table below). These rules follow a flexible approach establishing adequate duty of care for linking providers, which, in particular, involves a balancing of interests between the link providers, Internet users and rightsholders.[200]

Table 3. Selected EU caselaw concerning the liability of "linking" providers

Case reference	Key issue	CJEU's decision
C-466/12 *Svensson and Others*	Press articles written by several Swedish journalists were published on a freely accessible basis on the website of the *Göteborgs-Posten*. Retriever Sverige, a Swedish company, operates a website that provides its clients with hyperlinks to articles published on other websites, including the site of the *Göteborgs-Posten*. Retriever Sverige did not, however, ask the journalists concerned for authorisation to establish hyperlinks to the articles published on the site of the *Göteborgs-Posten*. The question was raised before the CJEU as to whether the provision of hyperlinks to copyrighted content that is freely available elsewhere is a form of communication to the public?	The CJEU decided that the owner of a website may, without the authorisation of the copyright holders, redirect Internet users, via hyperlinks, to protected works available on a freely accessible basis on another site. This is so, even if the Internet users who click on the link have the impression that the work is appearing on the site that contains the link.
C-160/15 *GS Media/Sanoma*	GS Media operates the website GeenStijl, a Dutch blog that publishes news, revelations and journalism, and which is reported to be one of the ten most visited sites in the Netherlands. In 2011, GeenStijl published an article and a hyperlink directing viewers to an Australian website where photos of Ms Dekker were made available. Those photos were published on the Australian website without the consent of Sanoma, the editor of the magazine Playboy, which holds the copyright to the photos. Despite Sanoma's demands, GS Media refused to remove the hyperlink. When the Australian website removed the photos at Sanoma's request, GeenStijl published a new article that also contained a hyperlink to another	The CJEU decided that the posting on a website of a hyperlink to works protected by copyright and published without the author's consent on another website does not constitute a "communication to the public" when the person who posts that link does not seek financial gain and acts without knowledge that those works have been published illegally. In contrast, if those hyperlinks are provided for profit, knowledge of the illegality of the publication

http://curia.europa.eu/juris/document/document.jsf?docid=83961&doclang=en.

[200] For further details about related case-law, see Cabrera Blázquez F., Cappello M., Grece C., Valais, S., *Copyright enforcement online: policies and mechanisms*, IRIS Plus, *op. cit.*

	website on which the photos in question could be seen. That site also complied with Sanoma's request that it remove the photos. Internet users visiting the GeenStijl forum then posted new links to other websites where the photos could be viewed. The question was raised before the CJEU as to whether hyperlinking to a public third-party website that contains work(s) published without the consent of the rightsholder constitutes a "communication to the public" within the meaning of the Copyright Directive (2001/29/EC)?	on the other website must be presumed.
C-527/15 *Stichting Brein*	Mr Wullems sells various models of a multimedia player under the name "filmspeler" over the Internet. This device acts as a medium between a source of audiovisual data and a television screen. Mr Wullems installed on the player an open source software that enabled files to be played through a user-friendly interface, via structured menus. In addition, integrated into the player were add-ons available on the Internet whose function was to retrieve the desired content from streaming websites and make it start playing on the multimedia player connected to a television at the click of a button. Some of those Internet sites give access to digital content without the consent of rightsholders. Stichting Brein, a Dutch foundation for the protection of rightsholders' interests, asked Midden-Nederland District Court to order Mr Wullems to cease selling multimedia players or offers of hyperlinks that illegally give users access to protected works. Stichting Brein submitted that, by marketing the multimedia player in question, Mr Wullems had made a 'communication to the public' in breach of the Dutch law on copyright which transposed Directive 2001/29. The Dutch court decided to refer a question on that subject to the CJEU.	The CJEU held that the sale of a multimedia player which enables films that are available illegally on the Internet to be viewed easily and for free on a television screen could constitute an infringement of copyright. The Court also found that temporary acts of reproduction on that multimedia player of a copyright-protected work obtained by streaming on a website belonging to a third party offering that work without the rightsholder's consent, cannot be exempted from the right of reproduction.
C- 610/15 *Ziggo/Brein ("the PirateBay")*	Ziggo and XS4ALL are Internet access providers. A significant number of their subscribers use the online sharing platform	The CJEU decided that making available and managing an online platform

	"The Pirate Bay". This platform allows users to share and upload, in segments ('torrents'), works present on their computers. The files in question are, for the most part, copyright-protected works in respect of which the rightsholders have not given the operators or users of that platform consent to share those works. Stichting Brein, a Dutch foundation which safeguards the interests of rightsholders, brought proceedings before the courts in the Netherlands seeking an order that would require Ziggo and XS4ALL to block the domain names and IP addresses of "The Pirate Bay". The Dutch Supreme Court decided to refer the questions as to whether a sharing platform is making a "communication to the public" within the meaning of the Copyright Directive and therefore infringing copyright?	for sharing copyright-protected works, such as "The Pirate Bay", may constitute an infringement of copyright. Even if the works in question are placed online by the users of the online sharing platform, the operators of that platform play an essential role in making those works available.

5.2.2.4 Secondary liability of information society services

Even if they benefit from the liability exemption privilege under the ECD, and despite the fact that Article 15(1) of the same directive prevents member states from imposing on information society services a general obligation to monitor, specific injunctions are, in principle, allowed against them (Article 12(3) and Article 15(2) of the directive).[201] Based on these provisions, rightsholders can ask them to take measures to prevent future rights infringement. This can establish duties of care by information society services, for example, filtering duties by hosting providers or blocking duties by access providers.

The CJEU, in some ground-breaking cases, made a clear distinction between filtering measures which are used to detect copyright infringements but which require some form of preventive monitoring of networks, and blocking measures, which basically prevent access to copyrighted material.[202]

[201] Article 15 of the E-Commerce Directive on "No general obligation to monitor" applies in particular to injunction claims which are raised pursuant to Article 8(3) of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights and Article 11 third sentence of Directive 2004/48/EC on the enforcement of intellectual property rights, the Enforcement Directive, which provide that member states shall ensure that rightsholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right or an intellectual property right.

[202] See Angelopoulos C., "Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post-Telekabel EU legal landscape", Journal of Intellectual Property Law & Practice, 2014, Vol. 9, No. 10, http://jiplp.oxfordjournals.org/content/9/10/812.

Table 4. Selected EU caselaw concerning secondary liability of information society services (ISS)

Case reference	Key issue	CJEU's decision
Case C-70/10 *Scarlett Extended v SABAM*	In 2004, the Belgian collective management society SABAM established that users of Scarlet's services were downloading works in SABAM's catalogue from the Internet, without authorisation and without paying royalties, by means of peer-to-peer networks. In the first instance, the Brussels Court ordered Scarlet, in its capacity as an ISS, to bring those copyright infringements to an end by making it impossible for its customers to send or receive in any way electronic files containing a musical work in SABAM's repertoire by means of peer-to-peer software. Upon appeal of the sentence by Scarlett, the Appeal Court asked the CJEU whether EU law permits member states to authorise a national court to order an ISP to install, on a general basis, as a preventive measure, exclusively at its own expense and for an unlimited period, a system for filtering all electronic communications in order to identify illegal file downloads.	The CJEU precluded the imposition of an injunction by a national court which requires an ISS to install a filtering system with a view to preventing the illegal downloading of files. Such an injunction does not comply with the prohibition on imposing a general monitoring obligation on such a provider, or with the requirement to strike a fair balance between, on the one hand, the right to intellectual property, and, on the other, the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information.
C-360/10 *Sabam/Netlog*	SABAM had an objection to Netlog NV, which runs an online social networking platform where every person who registers acquires a personal "profile", which enables them to make use of the musical and audiovisual works in SABAM's repertoire without consent nor payment of royalties. SABAM requested the Brussels Court of First Instance to issue an injunction against Netlog. The court made a reference to the CJEU for a preliminary ruling to ask whether EU law precludes a national court from issuing an injunction against a hosting service provider, such as an	The CJEU found that the owner of an online social network cannot be obliged to install a general filtering system, covering all its users, in order to prevent the unlawful use of musical and audiovisual work. Such an obligation would not respect the prohibition to impose on that provider a general obligation to monitor nor the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart

	owner of an online social network, which requires it to install a system for filtering information stored on its servers by its service users, which applies indiscriminately to all of those users, as a preventive measure, exclusively at its expenses and for an unlimited period.	information, on the other.
Case C-314/12 *UPC Telekabel Wien*	At the request of two companies holding the rights to two films, the Austrian courts prohibited UPC Telekabel Wien, an ISS established in Austria, from providing its customers with access to a website 'kino.to', from where these films could be viewed and downloaded without their consent. Initially, the *Handelsgericht Wien* prohibited UPC Telekabel from providing its customers with access to the infringing website. This prohibition was to be carried out, in particular, by blocking that site's domain name and current IP address, and any other IP address of that site of which UPC Telekabel might be aware. As an appeal court, the *Oberlandesgericht Wien* partially reversed the order of the court of first instance and held that UPC Telekabel had to be regarded solely as an intermediary, and could only be required, in the form of an obligation to achieve a particular result, to forbid its customers access to the website at issue, but that it had to remain free to decide on the means to be used. UPC Telekabel appealed to the *Oberster Gerichtshof* (Austrian Supreme Court), which referred to the CJEU for a preliminary ruling.	The CJEU judged that an ISP may be ordered to block its customers' access to a copyright-infringing website. Such an injunction and its enforcement must, however, ensure a fair balance between the fundamental rights concerned.
C-99/16 *McFadden/Sony Music*	This case concerned the application of the liability privilege to the operator of a shop which offers access to a Wi-Fi network free of charge to the public in relation to copyright infringements committed by users of that network.	The CJEU ruled that the operator of a shop who offers a Wi-Fi network free of charge to the public is not liable for copyright infringements committed by users of that network. However, such an operator may be required to password-protect its

		network in order to bring an end to, or prevent, such infringements.

It is also worth mentioning a recent case referred to the CJEU on 30 January 2018[203] by the Supreme Court of Austria (OGH) concerning the scope of Article 15(1) of the ECD and the liability privilege of hosting providers in case of hate speech. The CJEU judgement is eagerly awaited as it will enrich the jurisprudence of the ECtHR on the scope of the liability exemption of social media platforms in relation to hate speech posted by users and on the extent of the notion of "duty of care" by such platforms.

5.2.3 Online platforms and personal data

5.2.3.1 The "right to be forgotten" in online platforms

The CJEU addressed for the first time the issue of the protection of individuals with regards to the processing of their personal data on websites and the responsibility of Internet search engine operators in relation to this issue, through its judgment in the case C-131/12, *Google v. Agencia Española de Protección de Datos (AEPD)*.[204]

The case concerned a Spanish national who had filed a complaint against Google with the *Agencia Espanola de Proteccion de Datos* (Spanish Data Protection Agency, the AEPD) in order to require Google to remove or conceal personal data concerning him which appeared in a link to a Spanish newspaper provided by the search engine and which were no longer relevant, so that they no longer appeared in the search results. The AEPD upheld the complaint, as operators of search engines are subject to data protection legislation. Google brought an action against the decision before the National High Court, which referred a number of questions to the CJEU relating to (1) the territorial application of Directive 95/46 on the processing of personal data; (2) the activity of search engines as providers of content; and (3) the scope of the so-called "right to be forgotten".

The Court found that the activity of a search engine must be classified as "processing of personal data" when the processed information contains personal data. The operator of the search engine must be regarded as the "controller" in respect of that processing and - upon request - is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties, and containing information relating to that person.

[203] See Chapter 3 of this publication, Oberste Gerichtshof - OGH, Case 6Ob116/17b, https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20171025_OGH0002_0060OB00116_17B0000_000/JJT_20171025_OGH0002_0060OB00116_17B0000_000.pdf. See also, http://ipkitten.blogspot.fr/2018/01/austria-refers-facebook-hate-speech.html and http://merlin.obs.coe.int/iris/2018/3/article9.en.html.
[204] CJEU, 13 May 2014, C-131/12, *Google Spain v. AEPD and Mario Costeja Gonzalez,* http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

As regards the directive's territorial scope, the CJEU held that "processing of personal data" is carried out in the context of the activities of the controller being established on the territory of a member state when the operator of a search engine sets up a branch that is intended to promote and sell advertising, and that orientates its activity towards the inhabitants of that member state.

Finally, concerning the scope of the so-called "right to be forgotten", the Court established that if it is found, following a request by the data subject, that the inclusion of those links in the list is, at that point in time, incompatible with the directive, the links and information in the results must be erased. The Court observed in this regard that even the initially lawful processing of accurate data may, in the course of time, become incompatible with the directive. This is valid when, having regard to all the circumstances of the case, the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed. The Court added that, when appraising such a request made by the data subject in order to oppose the processing carried out by the operator of a search engine, the legitimacy of this request should be examined. In particular, consideration should be given to the question of whether the data subject has a right that the information in question relating to him personally should, at that point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name. If that is the case, the links to web pages containing that information must be removed from that list of results, unless there are particular reasons, such as the role played by the data subject in public life, justifying a preponderant interest of the public in having access to the information when such a search is made.

The Court pointed out that the data subject may address such a request directly to the operator of the search engine (the controller) who must then duly examine its merits. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly.

5.2.3.2 The transfer of personal data to third countries by online platforms

Another interesting judgment in relation to the processing of personal data by online platforms concerns the specific issue of the transfer of a person's data to a third country, which was addressed by the CJEU on 6 October 2015, through its judgment in Case C-362/14, *Schrems v. Data Protection Commissioner*.[205]

The case arose when an Austrian user of Facebook made a complaint to the Irish Data Protection Commissioner, asking the authority to prohibit Facebook Ireland from transferring his personal data to the United States, as he claimed that US law did not adequately protect his personal data. The Commissioner rejected the complaint, holding that under the Commission's Decision 2000/520 (the "safe harbour scheme"), US law

[205] CJEU, 6 October 2015, C-362/14, Maximilian Schrems v Data Protection Commissioner, http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:62014CJ0362.

ensured an adequate level of protection. The Irish High Court reviewed the Commissioner's decision, and asked the CJEU to rule on whether the Commissioner was absolutely bound by the Commission's decision on US law, and whether the Commissioner should instead carry out its own review of US law.

The CJEU ruled that the Data Protection Directive must be interpreted as meaning that a Commission decision "does not prevent" a national authority from examining a claim from an individual that "the law and practices in force" in another country "do not ensure an adequate level of protection". The Court then noted that the Irish court "seems essentially to share" the complainant's "doubts" about the "validity of Commission 2000/520", and "in order to give the referring court a full answer", the Court also examined whether the Commission's decision complied with the Data Protection Directive and the EU Charter of Fundamental Rights. The CJEU reviewed the Commission's decision, and concluded that the decision was "invalid" because "the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments". Thus, the decision was invalid, "without there being any need to examine the content of the safe harbour principles" by the Court. Finally, the Court held that the Commission "exceeded [its] power" when it restricted national authorities' powers of review.

5.2.4 Online platforms and the abuse of dominant position

From a competition law perspective, online platforms raise a number of new issues and enforcement challenges. The first of these questions concerns the very notion of "online platforms", its scope and limitations.[206] Once this notion has been defined, then comes the delimitation of the market in which such platforms operate (and whether online platforms primarily operate in a given market). Furthermore, the legal assessment of the market in question, from a competition law perspective, becomes more challenging due to the often multisided dimension of platforms which may evolve in several adjacent markets. In addition, new types of potentially anti-competitive practices may arise in the operation of online platforms, which relate, for example, to the exchange of sensitive business information or concerted practices, which are increasingly challenging for competition authorities to detect. Moreover, the assessment of market power can raise new questions and challenges too, considering the new role of big data, the parallel use of different services and switching costs for users, the significant importance of both direct and indirect network effects, etc. Finally, online platforms tend to strengthen competition in a

[206] See for example paragraph 45 and following of the *Facebook/WhatsApp* decision, where the European Commission defines the concept of social networking services: Case No COMP/M.7217 – *Facebook/WhatsApp* Regulation (EC) No. 139/2004, Merger procedure, Article 6(1)(b) Non-opposition, 3 October 2014, http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.

given sector and potentially introduce significant shifts in the balance of power in a determined market, which raises new competition law challenges.[207]

In view of these new challenges posed by the rise of dominant online platforms in the EU market, the objectives of the competition services of the European Commission have been to prevent the potential risks that such powerful platforms pose for businesses, users and society, while at the same time creating the best conditions for digital platforms to grow in Europe.

A large number of complaints have been received by the competition services of the European Commission on a wide range of allegedly anti-competitive practices by dominant online platforms, such as Google, Amazon, Facebook or Apple, in different areas of their business activities. For example, in the case of Google, complaints have been lodged by advertising platforms, telecom operators, publishers, associations of picture industries and photo libraries, etc. in relation to the following main broad allegations:[208]

- The use of Google's dominant position in searches to artificially display its own specialised services in a prominent manner to the detriment of rival services and without informing its users that such results do not result from the natural search engine;
- Advertising exclusivity and undue restrictions on advertisers;
- The imposition of exclusivity agreements on publishers – such as online newspapers – who want to use its search advertising intermediation programmes to display Google ads on their websites.
- Google's use of original content from other websites in its own web search services without consent (known as 'scraping').

For many of these alleged restrictions, Google cooperated with the European Commission during the antitrust investigation processes, through commitments to modify or remove anticompetitive conducts. However, in June 2017, the European Commission imposed a record fine of 2.42 billion euros on Google for unfairly directing users to its own products over those of its rivals.[209]

In the same way, in December 2017, the Spotify and Deezer CEOs – along with a group of European game companies – signed a letter to the European Commission President Jean-Claude Juncker calling the European Commission to ensure that they get a level playing field on platforms owned by large US technology companies, including Apple and Amazon. They called for *"clear and enforceable obligations that are deterrent and prevent unfair businesses practices by platforms"*. They consider that new EC regulation

[207] For further details, see, Hobbelen, H., Lorjé, N., and Guenay, A., "Selected recent developments in the application of EU competition law to online platforms", https://www.eui.eu/Projects/ENTRANCE/Documents/NewEntrance/Workshops/AnnualConference/Recent-Development-in-the-Application-of-EU-Competition-law-to-Online-Platforms-Hobbelen-Lorje%CC%81-Guenay.pdf.

[208] Other allegations regarding Google's activities are not related to antitrust, and include domains as diverse as corporate taxes, data privacy, copyright and net neutrality.

[209] http://europa.eu/rapid/press-release_IP-17-1784_en.htm.

should go *"beyond mere transparency requirements, which alone will not ensure platforms act as gateways rather than become gatekeepers to the digital economy."*[210] This initiative follows a first letter sent in May 2017 to the European Commission, in the context of the mid-term review of the Digital Strategy, to complain about online platforms – such as search engines and app stores – abusing their position as gateways to customers to promote their own services or impose imbalanced terms and conditions.

Another example of unfair practices may be illustrated by Google's alleged attempt to put pressure on independent music labels to extract better terms for its new streaming service on YouTube. In June 2014, IMPALA, the Independent Music Companies Association based in Brussels, lodged a detailed complaint with the European Commission, focusing on a series of breaches of European competition rules, and setting out five specific instances of conduct which IMPALA reported as illegal, given YouTube's position as a gatekeeper to the online market. IMPALA claimed, in particular, that YouTube was effectively creating artificial barriers to the accessing of the digital market and reported negotiating tactics consisting in the blocking of their artists' videos if they did not agree to sign up to non-negotiable contracts regarding YouTube's new premium subscription service. IMPALA reported the imposition by YouTube of abusive conditions to authors in relation to rights negotiations, as well as the imposition of abusive clauses in deals with video artists, such as the inclusion of a highly controversial 'least favoured nation' clause, provisions regarding the delivery of content that restrict the freedom of labels and their artists to decide on how to handle releases and marketing, such as exclusives, etc.[211]

5.3 Selected national case law

The present section presents a reasoned outline of selected national case law on topics that appear relevant for the issues concerning online platforms. The topics and countries included in the tables below should not be considered as an exhaustive overview, but rather as a structured exemplification of the most interesting developments in the last few years, as reported in the MERLIN Database of the Observatory[212] and integrated with further desk research.

The cases have been grouped into six clusters: 1) notion of platforms, 2) protection of minors, 3) protection of citizens, 4) advertising and the protection of consumers, 5) data protection and 6) protection of copyright. Within each thematic cluster, the cases are displayed by country, with a short summary of the concrete case and the main ruling of the judging court.

[210] https://www.presse-citron.net/streaming-deezer-spotify-accusent-apple-dabus-de-position-avantageuse/.

[211] http://www.completemusicupdate.com/article/impala-confirms-ec-complaint-submitted-over-youtube-dispute/.

[212] Access to the EAO MERLIN Database is available at http://merlin.obs.coe.int/.

5.3.1 On the notion of "platform"

As has been illustrated in previous sections, in the online environment, the commonly used notion of "platform" refers to and may cover a broad range of services (for example, Amazon, eBay, Facebook, Uber, etc.) and business models (for example, social media, search engines, app stores, e-commerce platforms, price comparison websites, etc.), which have little in common. Given how rapidly technological developments are evolving, it seems likely that this notion will remain blurry. As a consequence of scattered market concepts, the word "platform" itself has been used with different meanings in a variety of policy initiatives at both EU and national level. The legal definition of online platforms is quite a different matter, and this is clearly reflected in the court decisions that have been taken so far.

Table 5. Selected national case law concerning the notion of online platforms

Case reference	Key issues	Main ruling
DE – Germany		
Case Hotelbewertungsportal I ZR 94/13	Hotelbewertungsportal is a hotel review website that allows users to write reviews rating hotels. Following the publication of a comment stating "For €37.50 per person per night there were bedbugs", the hotel owner took legal action against the hotel review site, claiming damages.	In 2015, the German Federal Court of Justice found that the review site did not actively promote or disseminate the users' reviews and was not liable for the accuracy of user-generated ratings due to the intermediaries' liability exemption provided under Article 10 of the Telemedia Act transposing certain provisions of the e-Commerce Directive. The Court also noted that there was no obligation on the website to fulfil "any unreasonable duties to review," which could "challenge the entire business model" of the platform operator.
FR – France		
Pewterpassion et Saumon's v. Leguide.com 11-27729	Two companies, Pewterpassion and Saumon's, brought legal action against the price comparison website, Leguide.com, which offers priority referencing contracts to its users against payment, allowing them to top rank their products.	The French Supreme Court rejected the argument that this comparison website qualified as a mere hosting service provider and upheld the qualification of an advertising activity. Instead, the Court found that the platform, by top ranking products against remuneration by third-party traders, was indirectly promoting these products and thus acting as an active provider of a commercial service for these traders.
IT – Italy		
AGCM's decision on TripAdvisor Decision	TripAdvisor is an online platform that allows its users to publish reviews and compare hotels and restaurants with a view to sharing them with other users, thus providing advice on the locations	According to the Italian Competition Authority (AGCM), which examined the case in 2014, the fake reviews were considered as misleading information and unfair commercial practices, as they would have an impact on the

Case reference	Key issues	Main ruling
	listed in TripAdvisor. TripAdvisor uses a filtering system to check the truthfulness of reviews. However, it appeared that many fake reviews could be published in what would then be acts of unfair competition.	classification of the locations, distort competition, and deceive the average consumer, hence infringing Articles 5, 6 and 7 of the Unfair Commercial Practices Directive transposed into the Italian Consumer Code. Consequently, Tripadvisor was fined EUR 500 000 and was given 90 days to comply with the decision.
Natural person v. Google Italy Case no. 5107/14	The case is about a video published on Google video showing several youngsters bullying and making fun of a mentally handicapped classmate. In a criminal ruling by the Milan Court of First Instance in 2010, three Google executives received a six-month suspended prison sentence for privacy breaches. However, in December 2012, the Milan Court of Appeal overturned the first-instance ruling and acquitted them.	The Italian Supreme Court of Appeal, having taken into account the jurisprudence of the CJEU, ruled that Google should be classified as a hosting provider, since the platform merely provided storage space for videos uploaded by third parties and did not contribute to the content itself. In the Court's opinion, only the user uploading the content could be held liable for any infringements. A hosting provider is not liable as long as it promptly deletes or blocks access to unlawful content after knowing of its existence.

5.3.2 Protection of minors

In a converged media environment, minors enjoy special protection to preserve their mental, moral and physical development, not only under European and national legislation and public policy initiatives, but also under private initiatives from the different stakeholders.

As the cases below show, minors are protected not only as users and viewers of online content, but also as subjects featuring in content that could be viewed, shared or hosted online; this also covers the way they are portrayed, as in child pornography content, which is treated as a criminal offense under member states' national laws.

In online commercial communications, minors are protected from commercial material that might seek to take advantage of their vulnerability by exhorting them to purchase or to persuade their parents or other adults to buy the products that are advertised for them.

Table 6. Selected national case law concerning the protection of minors on online platforms

Case reference	Key issues	Main ruling
AT – Austria		
Disney Universe	On the "Disney Universe" website,	The Austrian Supreme Court did not find any

Case reference	Key issues	Main ruling
Case 4 Ob 95/13v	videos and DVD's, as well as online games and music, were marketed accompanied by slogans like "See your series on DVD" and "Get your cool soundtrack", and links were provided to the e-commerce website Amazon, where the DVD's and CD's could be purchased.	infringement of the Unfair Commercial Practices Directive, which prohibits a direct exhortation to children to buy or persuade their parents or other adults to buy the products advertised for them. The Court noted that an extra step was necessary between the invitation to purchase and the actual decision to buy, which can only be taken by the consumer and not the advertiser. The mere indication of the possibility to buy is therefore not a "direct exhortation".
DE – Germany		
The German Federation of Consumer Organisations v. Runes of Magic Case I ZR 34/12	The German Federation of Consumer Organisations reported advertisements for video game accessories for the online game "Runes of Magic". The advertisements using the slogans "Pimp your character" and "Grab the opportunity and give your arms and weapons a certain something" appeared in online forums. The plaintiff considered that the advertisements infringed the German Act against Unfair Competition, since they were written in a language likely to appeal to children, which might represent an exhortation to children to purchase the accessories.	The Federal Court of Justice established that advertising characterised by addressing individuals directly in the informal singular second person and by the use of terms typical of those used by children, including "popular Anglicisms", were sufficient to determine that children were targeted by the advertisement.
ES – Spain		
CAC action against child pornography websites Press release from CAC	The case concerned two websites in English offering free-to-view photographs of partly or totally nude girls who appeared to be underage. The first website, based in the United States and belonging to an online community specialised in artistic content, contained pictures of girls in lingerie, with some of the pictures including the address of the second website, which showed girls exhibiting their sexual organs, some of whom were in an explicit sexual act.	Following a complaint, the Catalan Audiovisual Council (CAC) examined the reported websites and their content. Given the characteristics of the graphic material and the fact that the girls featuring in the pictures appeared to be underage, the CAC concluded that the content could be classified as child pornography, which constitutes a breach of the Spanish Criminal Code, and therefore denounced the websites to both the state prosecution and to the Catalan police

5.3.3 Protection of citizens

The variety of issues covered by the following case law shows how broad the notion of protection of citizens can be interpreted by judges at national level, especially with regard to hate speech and violence online. Given that online operators, building on key decisions and jurisprudence, have developed a certain degree of awareness and put in place tools to deal promptly with unlawful content, most of the complaints are aimed at the direct perpetrators of infringements who initially create and/or upload the content.

Content featuring undeniable seriously harmful images or language is always tackled with extreme severity and ordered to be removed.

However, situations where the protection of citizens may collide with other rights, such as the right to freedom of information and freedom of artistic creation, are often subject to the Court's assessment of how far the limits to the freedom of expression can go.

Table 7. Selected national case law concerning the protection of citizens on online platforms

Case reference	Key issues	Main ruling
AT – Austria		
Eva Glawischnig-Piesczek v. Facebook 6Ob116/17b	Austrian MP Eva Glawischnig-Piesczek complained about a news article shared by the Facebook page of a private user's profile. The article comprised a photograph of the MP, where she is called, among other things, a "wretched traitor to her people" and a "corrupt oaf", who "has not earned a single cent through honest work in her entire life". Her party was also described as a "party of fascists". As the MP's request asking for the article to be deleted and for the user's real name and personal details to be disclosed was rejected by Facebook, the plaintiff brought the case before the Court of Vienna.	A preliminary injunction ordered Facebook to remove the disputed content and to delete any future uploads identical or similar in meaning to the original content, making them inaccessible worldwide. Following this decision, Facebook blocked access to the content, but only in Austria, and appealed the decision. A second instance court partly upheld the initial decision, as it conditioned the obligation imposed on Facebook of the platform having actual knowledge of the infringement, for example, via a subsequent notice. Following an appeal by both parties, the case was brought before the Austrian Supreme Court, who submitted questions to the CJEU (see section 2 of this chapter)
DE – Germany		
Natural person v. YouTube Case 3 U 71/13	A person who was previously sentenced for a fatal traffic accident complained about numerous media reports relating the accident which mentioned his identity and showed his face. The plaintiff took court action against YouTube, the platform hosting the videos, requesting the withdrawal of the	The right to freedom of expression and the public's right to information took precedence over the plaintiff's general right to privacy, as the Hamm Appeal Court ruled that YouTube was not obliged to remove the media reports relating the incident. Moreover, the Court considered that the disputed content was of public interest and

Case reference	Key issues	Main ruling
	videos.	did not defame the plaintiff, and that, in principle, users of the platform should be allowed to view and download the content, which was deemed to be lawful.
ES – Spain		
CAC notification to YouTube Press release from CAC	A YouTube user uploaded a video showing a person offering a beggar biscuits filled with toothpaste. Despite the removal of the video, it was observed that it had been uploaded a further four times by other users.	The media regulator of the Spanish region of Catalonia (CAC), requested the removal of all four copies of the illegal video from YouTube. The CAC estimated that the video violated the fundamental rights of a person, in particular the beggar's right to dignity.
CAC notification to YouTube Press release from CAC	Five videos inciting violence against women, including Cómo pegar a una mujer ("How to beat a woman"), were reported to the media regulator of the Spanish region of Catalonia (CAC). In parallel, the State Attorney in Barcelona opened investigation proceedings concerning this illegal content.	The CAC ordered YouTube to remove the content, which constituted a criminal offence under the Spanish Criminal Code. The regulator's instruction came after an investigation by the State Attorney of Barcelona following complaints. Consequently, YouTube removed the five videos that they were hosting.
FR – France		
UEJF and AIPJ v. Dieudonné Urgent procedure – 12 February 2014	The French comedian Dieudonné was ordered by a court decision to remove a video from his YouTube channel, where two sequences allegedly contained incitement to racial hatred and promoted crime against humanity - in reference to crimes committed during the Second World War. However, the unlawful content was duplicated by other users, including on other video platforms, and has been viewed more than 3 million times. YouTube, the content host, refused to remove the video unless the disputed content was declared illegal by court decision; and until the judgment was delivered, YouTube merely posted a warning message to users: "The following content has been identified by the YouTube community as being potentially offensive or inappropriate. Viewer discretion is advised."	A judge sitting in on urgent matters at the Paris Regional Court ordered Dieudonné to remove the content from his YouTube channel or risk paying a pecuniary fee per day which would correspond to the delay in doing so. The Court estimated that in the present case, the limits of freedom of expression had exceeded the degree of excess which could be tolerated.
LICRA v. Dieudonné, Les productions de la plume, et al.	A video entitled "Dieudonné the anti-Semite - the concentration camps" (in French), produced and directed by French comedian Dieudonné, could be viewed on the YouTube site to promote	The Paris Regional Court recalled that urgent procedure measures could only be ordered in extremely serious cases and only if there were serious elements that demonstrated the existence of a manifest danger of rights

Case reference	Key issues	Main ruling
Urgent procedure - 13 April 2012	the movie L'Antisémite. The disputed sequence, used for the trailer and shown at the start of the film, shows the arrival of an American officer, played by the comedian, discovering a concentration camp in 1945 as he is shown around by a former Jewish prisoner, who explains to him, in particular, how the gas chamber works. The civil society association LICRA appealed to the courts under urgent procedure for the withdrawal of the video and a ban on the film. The defendant maintained that the disputed video was no longer online, and that the movie was available only to subscribers to the defendant's official website. He also held that the film was covered by the right to freedom of expression, which allowed the use of parody, exaggeration and excessiveness.	infringement. Despite the provocative nature of the content, the Court thought the limits of freedom of expression had not been exceeded to such an extent as to justify a ban on the content, since it did not constitute an offence under law.
NL – The Netherlands		
Geert Wilders v. YouTube Case 09/837170-14	A Dutch musician published a music video clip on his YouTube account in March 2014 showing an actor imitating Dutch politician Geert Wilders being physically abused. The plaintiff complained about alleged threats. The musician's defence pleaded for acquittal on the grounds of freedom of expression and the right to use parody.	The Hague District Court estimated that Geert Wilders had reasonable grounds to fear for his life through the combination of the lyrics and the images where an actor is portraying the politician. The Court sentenced the musician to a suspended prison sentence and community work, and ordered the removal of the video clip accused of containing threats to a politician's lifeand of undermining his right to freedom of expression as well as his right to contribute to the public debate.

5.3.4 Advertising and the protection of consumers

While the legal status of video-sharing platforms is currently being reviewed under the revision of the AVMS Directive, cases regarding advertising and consumer protection are often dealt with through close cooperation between media regulators and the administrative bodies in charge of regulating advertising, media and the communication industries, especially when it comes to reporting content and identifying the potential risks related to commercial communication on consumers and on the market.

It is common knowledge that what makes online advertising so particular is: the interactivity it offers to the users it reaches, through hyperlinks, for example; the variety

of methods used to disseminate and display advertising messages; as well as the ability to share and republish content multiple times via the numerous websites and platforms. All these elements make the monitoring of online advertising and the enforcement of regulations more challenging, as becomes clearly apparent from the case law below.

Table 8. Selected national case law concerning advertising and the protection of consumers on online platforms

Case reference	Key issues	Main ruling
FR – France		
CSA notification to YouTube Press release from CSA	"Les recettes pompettes" is an entertainment programme produced by Studio Bagel Productions (Canal Plus) and broadcast via YouTube, where famous guests are invited to "cook and drink alcohol". The French Ministry of Health asked the programme's producers not to broadcast the first episode, claiming that it "encouraged excessive consumption of alcohol", before referring the matter to the Professional Advertising Regulatory Authority.	The French media regulator (CSA) confirmed that a YouTube channel qualifies as an on-demand audiovisual media service and falls under the scope of the on-demand audiovisual media service regime defined in Article 2 of the Law of 30 September 1986. CSA issued a warning as it considered that the content presents alcohol in a manner likely to encourage its consumption. Following this warning, Studio Bagel uploaded several episodes of the show featuring the following announcements at the beginning of the programme: "This programme contains subjects and situations that may not be suitable for young viewers the presence of a responsible adult is advised. Alcohol abuse can damage your health, consume with moderation".
GB – United Kingdom		
Oreo advertising in YouTube videos Ruling of ASA	The case concerned five YouTube channels owned by well-known private "vloggers" who humorously portrayed a particular way of eating Oreo biscuits. Following a complaint, the product manufacturer, Mondelez UK Ltd, admitted that these videos were part of a marketing project run in cooperation with the vloggers. However, it said that it had insisted that the vloggers make the marketing intent clear to the audience, which they had done, by including an in-video acknowledgement of the collaboration.	The British advertising authority (ASA) classified the videos concerned as advertising and drew a comparison with sponsorship, where a provider retained editorial control over its content despite receiving financial support. In the cases at hand, however, the owners of the YouTube channels had given editorial control over the advertising videos to the advertiser. ASA found that the labelling obligations for the advertisements contained in the videos had not been fulfilled properly and ordered the product's manufacturer to ensure that future advertisements make their commercial intent clear prior to consumer engagement. Claims of commercial collaboration are required to be included in a sufficiently clear manner and within an appropriate time limit, where these claims are part of the video.

5.3.5 Data protection

Most of the selected cases involving data protection concerned data processing by Internet service providers, mainly social media belonging to tech companies. The latest legal developments surely confirm the clear intent of European lawmakers to tackle the illegal processing of personal data and to ensure that such processing respects the standards set and required under EU and national legislation. Recent court and policy decisions show the complexity of taking appropriate action against intermediaries and online service providers, particularly considering the legal uncertainties as to where sometimes their accountability should stand.

The second most common situation where data protection is brought before courts is for the disclosure of data for the purpose of seeking legal action. By looking at the decisions, it can be noted that judges have systematically given priority to the right to seek legal action over editorial confidentiality in cases where this information has been deemed necessary to pursue legal procedures.

Table 9. Selected national case law concerning data protection on online platforms

Case reference	Key issues	Main ruling
AT – Austria		
Natural person v. Internet forum Gz. 6Ob133/13x	A Dutch politician requested the removal of Internet posts about himself, which he claimed to be offensive, and the disclosure of the e-mail addresses of the users who posted the comments. The operator of the forum deleted the comments, but refused to disclose the information requested on the grounds of editorial confidentiality, under the Austrian Media Act.	The Austrian Supreme Court endorsed an earlier ruling which considered that editorial confidentiality under the Austrian Media Act was inapplicable, since this provision, which guarantees the protection of journalists' sources, only applies to journalistic activities. The court held that the mere act of operating an online forum where all users are able to publish comments without moderation did not constitute any form of journalistic activity. The plaintiff's right to take action against the "website operator" (Betreiber der Website) to which the defendant had referred, was therefore insufficient, since the perpetrator could simply switch to another Internet site and continue infringing the plaintiff's rights, the Court concluded.
The Austrian Constitutional Court on the disclosure of an IP Address to the Security Police Case B 1031/11-20	The user of an Internet chat site had given the impression that he was offering underage children "7-11 years old or even younger if required" for sex. After being informed of this matter, the Vienna police authorities took immediate steps to collect the name and address of the person from the ISP, via the IP address that had been used to send the message.	The Austrian Constitutional Court rejected the complaint, as it considered that the police authorities were entitled to investigate the IP address simply on the grounds of a complaint brought to their attention either by a communication partner or by an open Internet communication service accessible to anyone. Although the right to data protection had been breached, this had taken place on a specific legal basis that was held entirely reasonable,

Case reference	Key issues	Main ruling
	The man initiated legal proceedings to complain that no judicial warrant had been granted before the data had been accessed and therefore claimed breaches of telecommunications secrecy and of the right to data protection under Austrian law.	in view of the reported behaviour.
BE – Belgium		
Belgian Privacy Commission v. Facebook Nr. AR/2016/153/A	The Belgian Privacy Commission started court proceedings against Facebook in 2015, following a study revealing that Facebook had tracked non-users and logged-out users for advertising purposes through "data cookies" on third-party websites. The proceedings resulted in a judgment by the Brussels Court of Appeal that found that the Belgian courts did not have jurisdiction over Facebook.	In 2018, the Brussels Court of First Instance established its jurisdiction over Facebook by drawing an analogy with the Court of Justice of the European Union's Google Spain case. The Court considered that it was Facebook Ireland's responsibility to ensure Facebook Belgium's compliance with national legislation regarding the processing of personal data. The Court found that Facebook's use of cookies, social plug-ins and "pixels" on third-party websites to track browsing behaviour were in violation of Belgian privacy law, especially since it was established that Facebook had not adequately inform users about the collection of data in the conditions mentioned above. In its decision, the Court ordered Facebook to destroy all personal data it had illegitimately obtained; to halt all third-party tracking of individuals browsing from Belgium until the company's policy conformed to Belgian privacy regulations; and finally, to publish the entire judgment on its own website, and the last three pages in both French and Dutch Belgian newspapers. Non-compliance with this order would result in the imposition of a daily fine of EUR 250 000, up to a maximum fine of EUR 100 million.
DE – Germany		
The German Competition Authority Background information	The German Competition Authority conducted a preliminary legal assessment of Facebook's collection and use of data from third-party sources as an abuse of a dominant position. The proceeding focused on the collection from third-party sources, such as services owned by Facebook (WhatsApp or Instagram), and websites and apps of other operators that are embedded into Facebook, but did not focus on the social network itself.	The proceeding concluded that Facebook's terms of service are inappropriate and violate data protection provisions to the disadvantage of its users. Moreover, and in view of the company's dominant position, the users' effective consent to this form of data collection and processing cannot be considered to be done in an appropriate manner.

Case reference	Key issues	Main ruling
	This administrative proceeding aimed at offering Facebook a chance to react to the allegations, to submit justification for its conduct and to provide for potential solutions and remedies. The follow-up on this matter is not expected before early summer 2018.	
IE – Ireland		
Muwema v. Facebook [2017] IEHC 69	The plaintiff complained about three allegedly "highly offensive and defamatory publications" posted on a Facebook page in March 2016 by a person identified under the pseudonym "Tom Voltaire Okwalinga" (TVO). As Facebook rejected the plaintiff's request, the latter addressed the issue to Court.	The High Court ordered the disclosure of the identity and location of the person(s) operating the Facebook page. However, it refused the injunctions sought under the Irish Defamation Act of 2009, instructing Facebook to "take down" the published content and to prevent its further publication. To justify its decision, the Court acknowledged the existence of multiple articles elsewhere on the Internet that were similar to the disputed article, including interviews where the plaintiff himself had discussed the allegations subject to the defamation complaint. In 2017, the High Court reversed the decision instructing the disclosure of the identity and location of the person operating the Facebook page; identified as a political activist, based on claims communicated by Facebook, revealing this person's identity could potentially pose a risk to his/her safety.
NL – Netherlands		
Data Protection Authority, lawfulness of the online enforcement of intellectual property rights by Dutch FilmWorks B.V. z2017-02053	Dutch FilmWorks B.V. (DFW), a Dutch film producer, notified the Dutch Data Protection Authority of its intention to instruct a data company to collect and process personal data for the purpose of copyright enforcement online. Such data processing would include the capturing of Dutch IP addresses to determine whether users of these addresses were involved in the distribution or reproduction of works protected by copyright, without informing the persons to whom the data relate about such processing.	The Dutch Data Protection Authority considered that the processing of data based on the subjects' alleged infringement of copyright amounted to the processing of criminal data. Moreover, the Authority estimated that the proposed processing met subsidiarity and proportionality standards, such as periodically deleting data at each stage of investigation. The Authority required that the persons to whom the data relate be informed about the processing of their data as soon as possible.
Natural person v. Google C/09/515777/ HA RK 16-377	A real estate entrepreneur against whom a criminal investigation had been conducted for mortgage fraud complained about news articles appearing when the applicant's name was entered in Google's search engine. The applicant based his request	The Hague District Court considered that Google had not processed personal data on criminal offences, as the three search results did not contain information which gave rise to a presumption more serious than a reasonable suspicion of committing a criminal offence, and thus rejected the plaintiff's claim.

Case reference	Key issues	Main ruling
	primarily on the grounds of the unlawful processing of personal data on criminal offences foreseen by the Dutch Data Protection Act.	The Court estimated that the right to freedom of expression and information should prevail over the applicant's "right to be forgotten", especially since fraud in the real estate sector and property development is part of a public debate. Moreover, the news articles to which Google linked were caused by the applicant's own behaviour, the Court added.

5.3.6 Protection of copyright

Decisions made by national courts reflect the national implementation of the e-Commerce Directive, allowing information society services to benefit from the liability exemption provided therein. According to this special regime, Internet service providers are not required to ensure proactive/ex ante control over third-party uploaded content (user-generated content). In most of the complaints, plaintiffs claimed that the service providers played an active role, which would trigger their liability.

In general, the organisation of content and the sale of advertising space were not considered such as to justify any claim of editorial responsibility, according to Court rulings. However, not acting promptly to remove infringing content, as required under Article 14 of the e-Commerce Directive, is sufficient to trigger the service provider's liability. Liability would also be held in case of repeated infringement, wherever the service fails to prevent further access to content previously withdrawn. It is therefore the responsibility of the rightsholders to report infringing content with sufficient precision as to help the service provider identify and take the appropriate action against such content.

The liability exemption regime set out by Article 14(1) of the e-Commerce Directive does not prevent member states from taking any appropriate measures, such as injunction orders, against intermediaries, in case of urgent matters, and in accordance with their legal systems.

Table 10. Selected national case law concerning the protection of copyright on online platforms

Case reference	Key issues	Main ruling
DE – Germany		
GEMA v. YouTube[213] Case 29 U 2798/15 **2012 ruling:** Case 310 O 461/10	The German music performing rights society (GEMA), complained to YouTube about copyright-protected music in videos hosted on its platform. By allowing such content to be published, YouTube would either be considered as a perpetrator of copyright violations, or be considered as a music service and would accordingly be obliged to pay licence fees. YouTube, on the other hand, mainly considered itself as a technical service provider with no control over the publication of audiovisual content by its users.	The Munich Higher Regional Court ruled that YouTube was not a music service subject to paying licensing fees to the music rights management society. In its view, the responsibility for the alleged copyright breaches lies with the users who upload the content and not with the platform itself. In a 2012 ruling, the Court of Hamburg considered that YouTube had not fulfilled its obligation to take prompt action to remove the copyright-breaching content, as it had taken one and a half months to do so, following a complaint by GEMA. Moreover, the Court found that YouTube had further review and control obligations, such as using a so-called Content ID tool, and should also, in future, install a word filter to prevent repeated breaches. In November 2016, and following years of legal discussions and negotiations, GEMA and YouTube reached an agreement on the remuneration for music content displayed on YouTube.
YouTube channel "Nitro Shqip" Decision 6 U 114/13	The copyright owner of the film "Sara's Show 46" filed a complaint against the operator of the YouTube channel "Nitro Shqip" for publishing a video in which excerpts of the film are shown and briefly commented on. The judgment deals essentially with the conditions in which the quotation right under German law applies.	The Cologne Court of Appeal ruled that distributing excerpts of a protected film for the purpose of criticism was considered contrary to German copyright law and did not fall under the right to quotation. The Court held that the freedom to quote should not be exploited as a vehicle for publishing a work or parts of it, adding that it is insufficient to insert or add quotations in an unstructured way; quotations should be closely related to the ideas being expressed by the person using them in order to be covered by the quotation right.
German Federal Supreme Court on Rapidshare Case. I ZR 80/12	The German music performing rights society (GEMA), issued a caution about a large number of music titles stored by the file-hosting service Rapidshare. Despite the caution, the provider did not completely remove the disputed files.	In a 2013 ruling, the German Federal Supreme Court confirmed that the service provider did not have a general obligation to monitor the stored data. However, depending on the specificities of each case, a monitoring obligation might apply. The Court noted that since Rapidshare could

[213] In similar terms, see also Natural person (Music producer) v. YouTube, Court of Hamburg, Case 308 O 27/09, https://openjur.de/u/590065.html.

Case reference	Key issues	Main ruling
		also be used for lawful purposes, it would not be expected to monitor everything with no specific reason, but only upon being notified about a potential infringement. The Court estimated that the fact that the service could be used anonymously would increase the risk of its service being used illegally. It also pointed to some indicators that would determine a potential infringement, such as the high number of downloads for a file, which Rapidshare would use to advertise its hosting service. The Court considered that, under such circumstances, the hosting provider should be expected to be subject to a partly-proactive monitoring obligation.
ES – Spain		
Telecinco v. YouTube Judgment N° 11/2014 **2010 ruling:** Judgment 289/2010	The Spanish private TV broadcaster Telecinco claimed that YouTube communicated content produced by Telecinco, illegally and without prior authorisation, to the public. The plaintiff considered that YouTube was operating as a content provider and was therefore playing more than a passive role by classifying the most popular videos into different categories. YouTube retorted that it merely acts as an intermediary between users uploading videos and users viewing them and has no control over the content.	The Civil Provincial Court of Madrid found that the plaintiff's cease and desist letters did not contain sufficiently detailed information to enable the identification of the content. Also, the classification of the most popular videos into different categories does not constitute an active involvement in the provided content. In a first ruling in 2010, the Madrid Commercial Court saw the lawsuit rejected. As a content- hosting intermediary, YouTube cannot be forced to exert *ex ante* control over user-generated content. The decision stated that it was the rightsholder's responsibility to track the content uploaded onto YouTube and report it, providing copyright holders with a "content ID", a tool that allows them to protect their content automatically by blocking videos from being uploaded to the platform.
FR – France		
LFP v. Puerto 80 Project Decision 15/15968	The Internet streaming website Rojadirecta was offering live or slightly delayed broadcasts of sports events free of charge by displaying a calendar with a series of hypertext links which enabled the viewing of football games from the French league, organised by the French football league (LFP). The latter, having granted exclusive live audiovisual rights to pay-TV channels, contacted the website asking for the infringing content to be removed and to be prevented from reappearing again on the website.	The Regional Court of Paris found that the LFP was entitled to take action since it had a substantial pecuniary interest in preserving the exclusive nature of the sale of its rights to its commercial partners without unfair competition from the free-of-charge broadcasting operated by Rojadirecta. It also observed that, despite operating as a forum, Rojadirecta appeared to be knowingly and intentionally making an editorial choice, with a programme and an appropriate search engine, in such a way that users could have access to protected content.

Case reference	Key issues	Main ruling
	The defendant claimed it was merely a host, and therefore covered by the limited liability scheme provided for under the e-commerce Directive and the French law transposing it.[214]	By considering the website's editorial responsibility, the Court found the website guilty of copyright infringement. The website was ordered to delete and stop any hyperlinks allowing the viewing of LFP games and to pay a pecuniary fee for the moral and economical prejudice, in addition to paying legal fees and expenses.
SARL 120 Films and La chauve-souris v. Dailymotion Judgment	The producers of the film Sheitan complained to the video-sharing platform Dailymotion about five videos, corresponding to the entire film divided into five parts, hosted by the platform. Dailymotion withdrew the videos three months after having received the complaint.	A first ruling by the Regional Court of Paris in 2010 noted that Dailymotion could not benefit from the limited liability exemption under the e-Commerce Directive and the French law implementing it, since it had not "promptly" withdrawn the disputed content when it was reported by the producers. The Court also noted a repeated infringement of the intellectual property rights in the same work, since Dailymotion was unable to prevent further access to content previously withdrawn. The initial ruling found Dailymotion guilty of copyright infringement and ordered the payment of a pecuniary fine in damages. The Court of Appeal found that the prejudice suffered by the applicant production companies had been underestimated in the initial proceedings with regards to the damages suffered, due to the length of time the content had remained online. Thus, the Court of Appeal of Paris decided to raise the pecuniary compensation.
Omar Sy and Fred Testot v. Dailymotion[215] Decision 08/01375	Comedians Omar and Fred complained that their works had been put online on Dailymotion without their authorisation. The comedians argued that the platform was wrong in claiming the status of a provider of technical services because it made commercial use of the content by selling advertising space, the yield of which was directly correlated to the site's audience figures.	The Paris Court of Appeal found that the commercialisation of advertising space, as long as it does not induce a capacity of action of the service (of the video-sharing platform) on the contents put on line, is not of a nature to justify the qualification of editor of the service in question. The Court noted more specifically that there was no relationship between the method of remuneration by advertising and the content

[214] Loi N° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164.

[215] In similar terms see also Nord-Ouest Production, *C. Carion et UGC Images v. Dailymotion*, Cour de Cassation, Judgment 09-67.896, www.courdecassation.fr/jurisprudence_2/premiere_chambre_civile_568/165_17_19033.html and *Flach Film and Editions Montparnasse v. Google*, Court of Appeal of Paris, Decision 12/82654, www.legalis.net/jurisprudences/tribunal-de-commerce-de-paris-8eme-chambre-jugement-du-20-fevrier-2008/.

Case reference	Key issues	Main ruling
		put on line, in such a way as to gain advantage or to carry out a selection of content that would enable targeted advertising. However, not acting promptly to remove copyright-infringing content resulted in the payment of a fee in damages, in respect of the moral and pecuniary prejudice suffered by the rightsholders.
IT – Italy		
RTI v. Break Media Decision 2833/2017	Break Media is an online video platform featuring content created by the platform itself or uploaded by its users. The platform was reported for violating broadcaster RTI's copyright by allowing videos of TV shows to remain online despite a cease-and-desist letter received from the rightsholder, which did not contain the URL to the unlawful content. The platform had editorial control over the content since it manually categorises videos on the basis of several criteria.	The Rome Court of First Instance considered that the platform should be classified as a content provider and not as a hosting provider, and therefore would not benefit from the liability exception provided by the e-Commerce Directive and the Italian law implementing it. It also clarified that a non-detailed cease-and-desist letter was sufficient to trigger the video platform's liability, as long as it highlighted the content in question with enough precision. The Rome Court of appeal confirmed the ruling issued by the First Instance Court sentencing the platform to pay a pecuniary fee as damages for reimbursement, in addition to legal fees and expenses.
AGCOM orders the disabling of access to IPTV pirate servers Decisions 223/17/CSP and 224/17/CSP	The case concerned two IPTV servers which provided access to a pirated service upon payment of a fee. Once their authenticity had been verified and the payment made, users were provided with a list of URLs granting them access to the livestreaming of copyright-protected programmes. In 2017, the rightsholder, Mediaset Premium S.p.A., complained to the Italian Communications Authority (AGCOM) about this infringement.	After examining the details of the case, AGCOM found that the websites used the service provider's logo to promote their illegal offers, and that the programmes made available were often among the search engines' first results, even as sponsored content, and were of good visual quality. AGCOM estimated that these factors might have led users to believe that this was a legitimate offer. Given this obvious copyright violation, AGCOM ordered the ISPs to disable access to the infringing websites within two days of the notification of the deliberations.
Delta TV v. YouTube Decision 1928/2017	The video-sharing platform YouTube was hosting copyright-protected audiovisual content owned by Delta TV whichhad been uploaded by the platform's users. Delta TV filed a notification asking the platform to withdraw the content published without authorisation, and an injunction was issued in 2014, ordering YouTube to take the necessary steps for the removal of the copyright-protected content.	The Court of Turin recalled the liability exemptions of ISPs, and ruled that an ISP is deemed to have actual knowledge of the existence of a copyright infringement once a specific and detailed notice of copyright infringement has been filed. The Court considered YouTube's actions to be insufficient, since the infringing content remained accessible; it held YouTube accountable for copyright infringement, and ordered it to pay a pecuniary fee in damages

Case reference	Key issues	Main ruling
	Instead of removing the unlawful content, the platform only blocked access to it in the plaintiff's country: Italy. Thus, the content then remained accessible from other locations or in Italy still, by using technologies that allow the IP address to be changed.	to the plaintiff.
AGCOM orders the disabling of access to pirated football games Decision n. 158/15/CSP	The case concerned several webpages hosted on servers managed by foreign companies which offered the possibility of viewing football games featuring Italian teams, whose audiovisual rights were owned by commercial broadcaster Mediaset.	Since the infringing website was hosted on servers located outside Italy, AGCOM reserved the right to order ISPs to disable access to the webpage within two days, and to redirect users seeking access to this website to a page stating that the infringing website was disabled due to copyright violation.
Mediaset v. Yahoo! Decision 3821/2011	The case was brought by Italian private TV broadcaster RTI (owned by the Mediaset group) against Yahoo! Italia. The latter was accused of displaying copyright-infringing content via its video-sharing platform. The platform provides a search tool that enables users to search for content by keyword; it indexes and selects videos; and it reserves the right to reproduce and adapt videos and to display them to the public, as well as the right to use them for promotional or advertising purposes, within its terms and conditions.	The Court of First Instance of Milan held that the liability exemption for hosting providers under the e-commerce Decree which implements the e-Commerce Directive did not apply to Yahoo! Italia, which was deemed to be an "active hosting provider" since it played an active role in organising its services and the videos uploaded to its platform with a view to commercial benefit. The Milan Court of Appeal rejected the distinction between "active" and "passive" hosting providers. It added that ISPs are liable only if they fail to remove the infringing contents upon receipt of a notice from the rightsholder or if they fail to comply with a removal order issued by the competent administrative or judicial authorities. A detailed cease-and-desist letter (which contains the URL where the infringing content can be found) sent by the rightsholder is equivalent to a removal order issued by the competent authority.
NL – Netherlands		
BREIN v. KPN, T-Mobile, TELE2, Zeelandnet and CAIW[216] C/16/448423/KG ZA 17-382	The dispute opposed BREIN, a foundation protecting the rights and interests of Dutch copyright holders, and five ISPs, namely T-Mobile, Tele2, CAIW, Zeelandnet and KPN, who were giving their end-users access to the notorious illegal downloading website The Pirate Bay.	The Midden-Nederland District Court based its decision on an earlier judgment from The Hague District Court, in the case opposing BREIN and ISPs Ziggo and XS4AALL. The Court acknowledged the "urgent nature" of the case. It also found that the blocking measures were justified, proportionate and effective, regardless of the fact that such

[216] Similar cases where ISP were ordered by national Courts to block access to The Pirate Bay can be noted, including: SCPP vs. Orange, Free et al. (FR), Dramatico Entertainment et al. vs. British Sky Broadcasting et al. (GB), EMI Records Ireland et al. vs. UPC Communications Ireland et al. (IE).

Case reference	Key issues	Main ruling
	BREIN requested the Court to order all ISPs to block access to the domain names and IP addresses through which The Pirate Bay operates.	measures can still be circumvented by the use of technical means, since the blocking would make it more difficult for end-users to access The Pirate Bay. All ISPs concerned would be required to pay a penalty fee in case of non-compliance with the decision.

6 State of play

6.1. Proposed measures in the context of the revision of the AVMSD

Following a complex REFIT exercise[217] and an extensive impact assessment[218] of all possible options as to the need for a revision of the AVMSD, the European Commission tabled a proposal for a revised AVMSD in May 2016. At the time of drafting this report, the debate had already been fed with various amendments from the co-deciding institutions, but the revision process had not yet been concluded.[219]

Video-sharing platforms are not covered by the current AVMSD, however they have been included in the scope of the AVMSD in the Commission proposal[220] with regard to the fight against hate speech and the dissemination of harmful content to minors. The provisions concern online platforms which organise and tag a large quantity of videos. According to the new wording, video-sharing platforms (VSPs) will have to put in place protection measures against harmful content within the limitations provided by the e-Commerce Directive. These new provisions build on existing efforts by the industry, and will be implemented by co-regulation.

The procedure that applies to the revision of the AVSMD is the Ordinary Legislative Procedure, formerly called co-decision procedure, whereby all three institutions act jointly and on an equal footing.

---

[217] European Commission, Ex-post REFIT evaluation of the Audiovisual Media Services Directive 2010/13/EU, https://ec.europa.eu/digital-single-market/en/news/ex-post-refit-evaluation-audiovisual-media-services-directive-201013eu.

[218] European Commission, Impact assessment accompanying the Proposal for an updated Audiovisual Media Services Directive, https://ec.europa.eu/digital-single-market/en/news/impact-assessment-accompanying-proposal-updated-audiovisual-media-services-directive.

[219] To follow the state of the art of the revision process of the Procedure file Procedure 2016/0151/COD, see the European Parliament's Legislative observatory, http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2016/0151(COD)&l=en and also the EUR-Lex, http://eur-lex.europa.eu/procedure/EN/2016_151.

[220] European Commission, Proposal for a directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016) 287 final, 25 May 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0287:FIN. For an overview see https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd.

At the moment of drafting the present report, the first reading had been concluded and the institutions are now involved in interinstitutional negotiations (so-called "trilogues") that have become standard practice for the adoption of EU legislation.[221] The aim of these trilogues is to agree on a common text, which can happen at any time.[222] The following sections will provide a brief overview of the most significant issues at stake, highlighting the main changes that have been proposed by the co-deciding institutions.

The current text takes into account the compromise agreement reached in 2017 and the outcome of the trilogue of 26 April 2018. A further trilogue will take place on 6 June to finalise the negotiations, which will be followed by a decision of the Council and the European Parliament's plenary vote. Once published in the Official Journal, the new rules will have to be transposed into national law by the member states.

6.1.1. The definition of a VSP and general principles

Article 1 (1) (aa) of the Commission proposal provides a definition of "video-sharing platform service", Article 1(da) provides a definition of "video-sharing platform provider" and Article 1(ba) provides a definition of "user-generated video". While both the Commission and the Parliament use the general and generic term "content", the Council provides a more detailed wording by mentioning the different types of content that can be found on a video-sharing platform, which are "programmes" or "user-generated videos".

The European Parliament includes a reference to video-sharing platforms and to user-generated videos in the definitions of "sponsorship" and "product placement" under Article 1 (1), points (k) and (m), respectively.

The compromise text of April 2018 provides detailed criteria for a service to be considered as a video-sharing platform under Compromise Article 1 (1) aa, according to which the principal purpose of the service or of a dissociable section of the service or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public.

Table 1 in the Annex to this publication gives an overview of the on-going revision process with regard to the provisions concerning the definition of video-sharing platforms and the general principles that are applicable to them.

[221] The trilogues are of an informal nature and are regulated by a Code of conduct for negotiating in the context of the Ordinary Legislative Procedures, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+RULES-EP+20130521+ANN-21+DOC+XML+V0//EN&language=EN&navigationBar=YES.
[222] European Parliament, Legislative train schedule, http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-audiovisual-media-framework.

6.1.2. The provisions applicable to VSPs

Article 28a of the Commission proposal includes certain obligations on the part of VSPs and the measures that they are expected to put in place to fulfil these obligations.

During the revision process, the obligation to protect citizens from harmful content containing incitement to violence or hatred was extended in Article 28a(1)(b) to include additional sets of groups – as well as to individuals belonging to these groups – with new criteria such as belief, disability, age and sexual orientation. Another proposed addition is the obligation to protect the general public from content "containing public provocation to commit a terrorist offence", under Article 28a(1)(ba) in the Council's general approach.

The Council also addresses, under a proposed Article 28a(1a), the liability of VSPs with regard to audiovisual commercial communications that are marketed, sold and arranged by those VSPs, but also those that are not marketed, sold and arranged by those VSP providers themselves, taking into account the limited control that the platforms have over such content. This last specification takes into account the liability regime under Article 14 of the e-Commerce Directive. This issue is also addressed by the Parliament under Article 28a(5a).

The proposal includes a list of measures aimed at empowering users, who, in practice and more than ever, are now important "partners" for the VSPs, as they use the flagging and reporting tools provided by the VSPs to tackle unlawful content. This way, users would contribute to fulfilling the obligations incumbent upon VSP providers, namely to put in place a set of tools (an obligation of means) that users should use in order to protect themselves (or their children) while using these services. In addition to these tools, and in order to make users' empowerment more effective, special attention is paid to:

- transparency and the two-way-communication between users and VSP providers under Article 28a(2)(f) and the Council's proposed Article 28a(2)(ba), by providing feedback to the reporting of content by users;
- media literacy, as member states are invited to encourage policies and schemes to develop media literacy skills;
- data protection under Article 28a(2)(c) of the Council's general approach, by ensuring that age verification systems do not lead to any additional processing of personal data and comply with the European data protection regulations, namely the Charter of Fundamental Rights of the European Union (CFREU), the General Data Protection Regulation (GDPR) and the Police Directive, and the new e-privacy Regulation which is expected to be adopted by the end of 2018.

The Compromise text of April 2018 refers to Articles 12 and 13 of the e-commerce Directive, respectively on mere conduit and on caching, as to the obligation for video-sharing platform providers to take appropriate measures to ensure a protected space for their users, under Compromise Article 28a (1). Compromise Article 28a (2) excludes any obligation of ex-ante control by video-sharing platform providers, in line with Article 15 of the e-Commerce Directive.

In addition to content inciting to commit a terrorist offence, video-sharing platform providers will be required under Compromise Article 28a (1)(ba) to fight content the dissemination of which constitutes a criminal offence under Union law, such as child pornography and content featuring racism and xenophobia.

As to user-generated videos, a new sub-paragraph (aaa) is added under Compromise Article 28a (2), which refers to measures enabling uploading users to declare whether, according to their knowledge, those videos contain audiovisual commercial communications. Users' rights are also reinforced, as the Compromise text guarantees under Compromise Article 28a (6a) the right to engage in judicial procedures in parallel with out-of-court complaint and redress mechanisms that are made available to solve disputes between users and video-sharing platform providers.

As to the protection of minors, the Compromise text forbids the data processing of minors' personal information for commercial communication purposes, under a paragraph which was added to Article 28a (2).

Table 2 in the Annex to this publication gives an overview of the on-going revision process with regard to the provisions concerning the obligations of video-sharing platforms.

6.1.3. The establishment of VSP providers

Article 28b of the Commission proposal provides the criteria to determine the member state of establishment of a VSP provider. The Council's general approach introduces a more detailed description of these criteria as it proposes definitions for "parent undertaking", "subsidiary undertaking" and "group".

The European Parliament endorses the Commission's initial proposal to allow VSP providers that have an effective presence in several member states, through several subsidiaries or entities of the group established in different member states, to elect their own member state of establishment. The Council, in its general approach, proposes a different view, as it suggests that the VSP provider be established in the member state where one of the subsidiaries or entities of the group first began its activity, provided that it maintains a stable and effective link with the economy of that member state.

The Compromise text of April 2018 adopts the wording of the Council's general approach, which includes the definitions of "parent undertaking", "subsidiary undertaking", and "group". Moreover, all undertakings having economic and legal organisational ties shall be considered as part of the same group of undertakings. Thus, a video-sharing platform provider shall be deemed to be established on the territory of a member state if it has economic and legal organisational ties to another undertaking that is established in that same member state.

Table 3 in the Annex to this publication gives an overview of the on-going revision process with regard to the provisions concerning the rules on establishment of video-sharing platforms.

6.1.4. The obligation to make certain information on VSPs accessible to users

The European Parliament proposes under a new Article 28c to extend to VSPs the obligation for audiovisual media service providers to make certain information accessible to the users, under Article 5 of the current AVMS Directive, including the name of the service provider; the geographical address where it is established; the contact details, including email address or website, which should make it possible to contact the VSP provider rapidly and in a direct and effective manner; and the competent regulatory or supervisory bodies, in addition to the member state of jurisdiction, as added under the proposal. However, this proposal was withdrawn in the Council's general approach.

The Compromise text of April 2018 contains no changes on this topic.

Table 4 in the Annex to this publication gives an overview of the on-going revision process with regard to the provisions concerning this obligation.

6.2. Proposed measures in the context of the Copyright Directive revision

On 14 September 2016, the European Commission published its proposal for a Directive on Copyright in the digital single market,[223] with the aim of modernising the current copyright framework, while taking into account the recent technological developments and the new ways of distributing copyright-protected content in the internal market.

This draft reform aims at fostering a better balance in the remuneration of the different actors in the value chain, as well as greater transparency in contractual arrangements between creators and online platforms and broader availability of copyright-protected content within and across EU borders.

Under this proposed Directive, and within the liability exemption provided by the e-Commerce Directive, Article 13[224] creates an obligation on information society service

[223] European Commission, Proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM(2016) 593 final, 14 September 2016, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2016:593:FIN. For an overview, see https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules.

[224] Article 13 (Use of protected content by information society service providers storing and giving access to large amounts of works and other subject matter uploaded by their users) of the Proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM(2016) 593 final

1. Information society service providers that store and provide the public with access to large amounts of works or other subject matter uploaded by their users shall, in cooperation with rightsholders, take measures to ensure the functioning of agreements concluded with rightsholders for the use of their works or other subject matter or to prevent the availability on their services of works or other subject matter identified by rightsholders through the cooperation with the service providers. Those measures, such as the use of effective content recognition technologies, shall be appropriate and proportionate. The service providers shall provide rightsholders with

providers storing and giving access to copyright-protected content uploaded by their users to take appropriate and proportionate measures to ensure that agreements concluded with rightsholders are duly respected, and to prevent the availability on their services of copyright-infringing content once it has been identified as such by rightsholders.

The negotiation of this Article has given rise to considerable controversy among stakeholders as to the consequences of the proposed measures on the obligations of information society service providers. It has been held that obliging service providers to put in place measures to *"prevent the availability on their services of works or other subject matter identified by rightsholders [...] such as the use of effective content recognition technologies"* would introduce a general monitoring obligation, and would therefore contradict the liability regime under Article 14 of the e-Commerce Directive, which has so far exempted information society service providers from such *ex ante* control over content.[225]

The proposal to oblige service providers to provide users with complaints and redress mechanisms in case of disputes over actions taken by the service providers on uploaded content has proved to be less controversial. These mechanisms would allow users to contest any potential disproportionate action taken by service providers, and to avoid cases where providers would address content on the basis of their terms of service, rather than on the basis of an effective breach of law, and regardless of users' right and freedom to disseminate content, even if such content is entirely legal.

The proposed Article 13 also sets the scene for future cooperation between information society service providers and rightsholders aimed at determining the so-called *"best practices, such as appropriate and proportionate content recognition technologies"*.

The procedure that applies to this legislative initiative is in the interinstitutional negotiations, and at the time of this publication the opinion of the European Parliament was still awaited.[226]

---

adequate information on the functioning and the deployment of the measures, as well as, when relevant, adequate reporting on the recognition and use of the works and other subject matter.

2. Member States shall ensure that the service providers referred to in paragraph 1 put in place complaints and redress mechanisms that are available to users in case of disputes over the application of the measures referred to in paragraph 1.

3. Member States shall facilitate, where appropriate, cooperation between the information society service providers and rightsholders through stakeholder dialogues to define best practices, such as appropriate and proportionate content recognition technologies, taking into account, among other things, the nature of the services, the availability of the technologies and their effectiveness in light of technological developments.

[225] See the open letter signed by 56 organisations against the proposed Article 13 at https://www.eff.org/files/2017/10/16/openletteroncopyrightdirective_final.pdf. For a critical comment see Angelopoulos C., EU Copyright Reform: Outside the Safe Harbours, Intermediary Liability Capsizes into Incoherence, Kluwer Copyright Blog, 6 October 2016, http://copyrightblog.kluweriplaw.com/2016/10/06/eu-copyright-reform-outside-safe-harbours-intermediary-liability-capsizes-incoherence/.

[226] To follow the state of the art of the revision process of the Procedure file 2016/0280/COD, see the European Parliament's Legislative observatory,

6.3. Initiatives in the context of the Digital Single Market Strategy

The Digital Single Market (DSM) Strategy for Europe, which was announced on 25 May 2016, refers to online platforms in several key actions recommended by the European Commission. However, rather than fixing a one-size-fits-all definition, the Commission has opted for a wide-ranging set of examples.[227]

6.3.1. The (non) revision of the e-Commerce Directive

The European Commission has been monitoring the effectiveness of the e-Commerce Directive in order to determine whether or not it suits the current technological evolution and the new ways of disseminating and viewing content online. For this purpose, it established an Expert Group, which held its first meeting in November 2005, and whose mission it was to advise the Commission on issues relating to electronic commerce and related services, with the clear objectives of enhancing/facilitating administrative co-operation between the member states themselves and between member states and the Commission; addressing problems in the application of the Directive; and discussing emerging issues in the field of e-commerce.[228]

In September 2015, as part of the DSM strategy, the European Commission launched a public consultation to assess the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy.[229] The consultation covered the social and economic role of online platforms; transparency; terms of use; rating systems and reviews; the use of information by platforms; and the role of online intermediaries, among other issues.

The observations emerging from the public consultation tend to indicate that, when it comes to online intermediaries & tackling illegal content online, certain concerns

---

http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2016/0280(COD)&l=en#keyEvents and also the EUR-Lex, http://eur-lex.europa.eu/procedure/EN/2016_280.

[227] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A Digital Single Market Strategy for Europe", SWD(2015) 100 final, COM(2015) 192 final, Brussels, 6 May 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=FR.

[228] The Expert Group on electronic commerce on the Register of the European Commission's expert groups, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=1636

[229] Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, from 24 September 2015 to 6 January 2016, https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud

It is also worth mentioning that a first public consultation on the future of e-commerce took place in 2010 (https://circabc.europa.eu/faces/jsp/extension/wai/navigation/container.jsp), followed by a public consultation on notice-and-action procedures in 2012 (http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet/summary-of-responses_en.pdf).

were raised regarding the current liability regime under the e-Commerce Directive. As highlighted in the responses, views are divided among those who consider that the actual regime still fulfils its purpose and those who advocate more clarification and guidance for its implementation, even suggesting the establishment of further categories of intermediary services, besides mere conduit, caching and hosting.[230]

The consultation showed a certain amount of support for the existing principles; consequently, the e-Commerce Directive is currently not undergoing any revision process.[231]

6.3.2. Initiatives on disinformation and "fake news"

The risks and the consequences of the increasing amount of "fake news" – or disinformation – online have been widely discussed over the past couple of years. As this phenomenon has reached global proportions, and in view of the threat that disinformation poses for democracy and public order, the European authorities have started to react and address this phenomenon.[232]

At EU level, a European Parliament resolution of 15 June 2017 on online platforms and the digital single market called on the Commission to analyse the current challenges and the actual legal framework in order to identify potential legal instruments to limit the dissemination and spreading of fake news content.[233]

In November 2017, the European Commission issued a Roadmap on "Fake news and online disinformation".[234] This roadmap aimed at involving stakeholders in any further action that would be taken by the Commission by informing them of the Commission's work, including the main problems and the potential solutions to be taken into account in any future steps, and collecting feedback from them.

In the same month, among the most significant recent initiatives, the Commission launched a public consultation on fake news and online disinformation and announced its intention to set up a High-Level Expert Group (HLG) representing academics, online platforms, news media and civil society organisations to help elaborate an EU-level

---

[230] European Commission, Full report on the results of the public consultation on the Regulatory environment for Platforms, Online Intermediaries and the Collaborative Economy, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15877.

[231] European Commission, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM(2016) 288 final, Brussels, 25 May 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288#footnoteref31.

[232] The United Nation's Office of the High Commissioner on Human Rights, via its Special Rapporteur on Freedom of opinion and expression, and the Organization for Security and Co-operation in Europe (OSCE), along with other international organisations issued a Joint Declaration on 'Fake News', Disinformation and Propaganda, in March 2017: www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E

[233] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0272+0+DOC+XML+V0//EN&language=GA.

[234] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-5489364_en.

strategy on how to tackle the dissemination and the spreading of fake news.[235] The HLG delivered its first report in March 2018.[236] The European Commission will build on this report as well as on the outcome of the public consultation on fake news and online disinformation[237] with the aim of publishing a Communication on tackling disinformation online.

The HLG's report identified a set of measures for online platforms in the short term. According to the report, online platforms should take part in a coalition along with news media outlets and civil society organisations, whereby all willing stakeholders from the relevant sectors would be involved in the process of elaborating the proposed multi-stakeholder Code of Practices and would accompany its implementation and continuous monitoring. This multi-stakeholder Code of Practices should set out concrete rules of conduct, taking into account the Key Principles set out by the HLG in its report which state that platforms should:

1. adapt their advertising policies, including adhering to a "follow-the-money" principle, through cooperation with the advertising industry to ensure that companies do not place ads on or host ads from companies identified for purveying disinformation;
2. ensure transparency and public accountability with regard to the processing of users' data for advertisement placements, with due respect for privacy, freedom of expression and media pluralism;
3. ensure that sponsored content, including political advertising, is appropriately identifiable from other content in order to guarantee transparency;
4. cooperate by enabling privacy-compliant access to data for the assessment of fact checking and for research activities;
5. make advanced settings and controls available to empower users and enable them to customise their online experience;
6. take effective measures, where appropriate and in cooperation with public and private European news outlets, to improve the visibility of reliable, trustworthy news and facilitate users' access to it;
7. ensure, where appropriate and if technically feasible, that trending news items are accompanied by related news suggestions;
8. provide, where appropriate, user-friendly tools to enable users to link up with trusted fact-checking sources and allow them to exercise their right to reply;
9. apply flagging and trust systems that rely on users, and design safeguards against their abuse by users;
10. cooperate by, *inter alia,* providing relevant data on the functioning of their services, including data for independent investigation by academic researchers

[235] The list of members of the GHLG can be found at https://ec.europa.eu/digital-single-market/en/news/experts-appointed-high-level-group-fake-news-and-online-disinformation.
[236] Report of the independent High level Group on fake news and online disinformation, March 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.
[237] Public consultation on fake news and online disinformation, from 13 November 2017 to 23 February 2018, https://ec.europa.eu/digital-single-market/en/news/public-consultation-fake-news-and-online-disinformation.

and general information on algorithms, in order to establish a common approach to address the dissemination and amplification of disinformation.

The HLG encouraged the adoption of a self-regulatory approach based on a clearly defined multi-stakeholder engagement process, including a set of short and medium-term actions, following a predefined roadmap for implementation. These short and medium-term measures would be followed by a proper evaluation of their effectiveness and efficiency. Based on this assessment, the European Commission would re-examine its approach in spring 2019 with a view to deciding whether further measures, including (co)regulatory interventions, competition instruments or mechanisms to ensure the continuous monitoring and evaluation of self-regulatory measures, should be considered for the next term. Furthermore, the European Commission listed the Communication on "Online platforms and fake news" in its Work Programme for 2018.

In parallel, the Council of Europe unveiled its report on “Information Disorder” at the end of September 2017.[238] The report identifies various types of information disorder, which are mis-information, mal-information and disinformation – an expression which, according to the authors of the study, best describes the complexity of the “fake news” and “information pollution” phenomena.

6.3.3. Initiatives concerning consumer protection

On 25 May 2018, the General Data Protection Regulation will come into force after being adopted on 24 May 2016 as part of the Digital Single Market Strategy. This Regulation would ensure the protection of natural persons with regard to the processing of personal data and the free movement of such data, with the aim of strengthening citizens' fundamental rights in the digital era, across the European Union and regardless of where the data is processed.

The Commission plans to extend and adapt EU law to new consumer practices of the digital age by introducing new rules to cover users of free-of-charge services like social networks and online platforms that use consumer data as a way of generating profit.[239] The proposed amendments would affect the Unfair Commercial Practices Directive and the Consumer Rights Directive, as well as the Unfair Contract Terms Directive and the Price Indication Directive. This proposal would acknowledge the

[238] Claire Wardle and Hossein Derakhshan, Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, Strasbourg, 27 September 2017, www.coe.int/en/web/freedom-expression/news/-/asset_publisher/thFVuWFiT2Lk/content/tackling-disinformation-in-the-global-media-environment-new-council-of-europe-report?_101_INSTANCE_thFVuWFiT2Lk_viewMode=view/&desktop=false.

[239] See Proposal for a Directive of the European Parliament and of the Council amending Council Directive 93/13/EEC, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules, COM(2018) 185 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0185.

increasing economic value of personal data, by it being monetised and used for an economic purpose, that is to say, for generating revenues from online advertising. This proposal would see the big Internet companies such as Google, Amazon, Facebook and Apple, to name but a few, comply with stricter measures or face high penalties in case of non-compliance. In this case, the amendments would envisage fines of up to 4 percent of the company's yearly revenue.

6.3.4. Initiatives concerning tax regimes

After publicly declaring their intention to address the tax regimes of giant tech companies, during the Economic and Financial Affairs Council (ECOFIN) meeting in September 2017, some EU member states agreed on introducing a new levy on digital companies. The Ministers of Finance and Economic Affairs of the EU member states admitted the need for EU-level action that would be more realistic and adapted to the market reality and to the effective profit generated by digital companies in the EU market in order to guarantee fair and equal taxation of companies, regardless of their location or place of activity. [240]

Member states identified two possible solutions, one based on "quick fixes" and the other on the principle of "virtual establishment": some member states proposed an "equalisation levy" on the turnover generated in Europe by digital companies, and another proposal suggested addressing the question of establishment upon which tax regimes are based. At the time of drafting this publication, no specific decision had yet been taken.

[240] Presidency Issues Note for the informal ECOFIN Tallinn, 16 September 2017, Discussion on corporate taxation challenges of the digital economy, www.eu2017.ee/sites/default/files/2017-09/Ecofin%20Informal_WS%20II_digital%20economy_15-16.Sept_.17.pdf.
See also https://www.euractiv.com/section/digital/news/eu-ready-to-hit-big-us-tech-firms-with-3-turnover-tax/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_recent_activity_details_shares%3BTCDHkIDNSCKTiIl6YziL3w%3D%3D.

7 Annex

Table 11. Revision process on definitions and general principles (Article 1 AVMSD)

Current AVMSD 2010/13/EU[241]	Commission proposal 25 May 2016[242]	EP amendments 10 May 2017[243]	Council Gen. Approach 23 May 2017[244]
	Article 1 (1) aa 'video-sharing platform service' means a service, as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, which meets the following requirements:	'video-sharing platform service' means a service, as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, which meets ***all*** the following requirements:	'video-sharing platform service' means a service, as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, which meets ***~~all~~*** the following requirements:
	Article 1 (1) aa ... (i) the service consists of the storage of a large amount of programmes or user-generated videos, for which the video-sharing platform provider does not have editorial responsibility;	(i) ***a main functionality of*** the service consists ***in making available*** of programmes or user-generated videos ***to the general public***, for which the video-sharing platform provider does not have editorial responsibility;	(i) ***the service consists of the storage of programmes or user-generated videos, for which the video-sharing platform provider does not have editorial responsibility;***
	Article 1 (1) aa ... (ii) the organisation of the stored content is determined by the provider of the service including by automatic means or algorithms, in particular by hosting, displaying, tagging and sequencing;	(ii) the organisation of the ***publicly made available content*** is determined by the provider of the service including by automatic means or algorithms, in particular by hosting, displaying, tagging and sequencing;	(ii) ***the organisation of the stored programmes or user-generated videos is determined by the video-sharing platform provider including by automatic means or algorithms, in particular by displaying, tagging and sequencing;***
	Article 1 (1) aa ... (iii) the principal purpose of the service or a dissociable section thereof is devoted to	(iii) the principal purpose ***of the service***, or of a service which is a dissociable	(iii) the principal purpose of the service, ***a dissociable section of that service or an***

[241] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013.
[242] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0287:FIN.
[243] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0192&language=EN.
[244] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9691_2017_INIT&from=EN.

Current AVMSD 2010/13/EU[241]	Commission proposal 25 May 2016[242]	EP amendments 10 May 2017[243]	Council Gen. Approach 23 May 2017[244]
	providing programmes and user-generated videos to the general public, in order to inform, entertain or educate;	section ***of a wider service***, is devoted to providing programmes and user-generated videos to the general public, in order to inform, entertain or educate, ***or that service plays a significant role in providing programmes and user-generated videos to the general public, in order to inform, entertain or educate; and***	***essential functionality of the service*** is devoted to providing programmes ***or*** user-generated videos to the general public, in order to inform, entertain or educate; and
	Article 1 (1) aa … (iv) the service is made available by electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC.	No amendment	No amendment
	Article 1 (1) ba 'user-generated video' means a set of moving images with or without sound constituting an individual item that is created and/or uploaded to a video-sharing platform by one or more users;	'user-generated video' means a set of moving images with or without sound constituting an individual item that is ~~***created and/or***~~ uploaded to a video-sharing platform ~~***by one or more users***~~;	'user- generated video' means a set of moving images with or without sound constituting an individual item, ***irrespective of its length, that is created by a user and uploaded to a video -sharing platform by that user or any other user***;
	Article 1 (1) da 'video-sharing platform provider' means the natural or legal person who provides a video-sharing platform service;	No amendment	No amendment
Article 1 (1) k 'sponsorship' means any contribution made by public or private undertakings or natural persons not engaged in providing audiovisual media services or in the production of audiovisual works, to the financing of audiovisual media services or programmes with a view to promoting their name, trade mark, image, activities or products;'	No amendment	'sponsorship' means any ***direct or indirect*** contribution made by public or private undertakings or natural persons not engaged in providing audiovisual media services, ***video-sharing platform services or user-generated videos*** or in the production of audiovisual works, to the financing of ***the*** audiovisual media services**, *or the video-sharing platform services, or the user-generated videos*** or the programmes with a view to promoting their name, trade mark, image, activities or products;'	'sponsorship' means any contribution made by public or private undertakings or natural persons not engaged in providing audiovisual media services or in the production of audiovisual works, to the financing of audiovisual media services or programmes with a view to promoting their name, trade mark, image, activities or products;
Article 1 (1) m 'product placement' means any form of audiovisual commercial communication	No amendment	'product placement' means any form of audiovisual commercial communication	'product placement' means any form of audiovisual commercial communication

Current AVMSD 2010/13/EU[241]	Commission proposal 25 May 2016[242]	EP amendments 10 May 2017[243]	Council Gen. Approach 23 May 2017[244]
consisting of the inclusion of or reference to a product, a service or the trade mark thereof so that it is featured within a programme, in return for payment or for similar consideration;		consisting of the inclusion of or reference to a product, a service or the trade mark thereof so that it is featured within a programme ***or a user-generated video***, in return for payment or for similar consideration	consisting of the inclusion of or reference to a product, a service or the trade mark thereof so that it is featured within a programme, in return for payment or for similar consideration;

Source: European Audiovisual Observatory elaboration on official EU documents.

Table 12. Revision process on provisions applicable to video-sharing platforms (Article 28a AVMSD)

Current AVMSD 2010/13/EU[245]	Commission proposal 25 May 2016[246]	EP amendments 10 May 2017[247]	Council Gen. Approach 23 May 2017[248]
	Article 28a (1) Without prejudice to Articles 14 and 15 of Directive 2000/31/EC, Member States shall ensure that video-sharing platform providers take appropriate measures to:	Without prejudice to Articles 14 and 15 of Directive 2000/31/EC, Member States shall ensure that video-sharing platform providers take appropriate***, proportionate and efficient*** measures to:	Without prejudice to Articles 14 and 15 of Directive 2000/31/EC, Member States shall ensure that video-sharing platform providers ***under their jurisdiction*** take appropriate~~***, proportionate and efficient***~~ measures to:
	Article 28a (1)(a) protect minors from content which may impair their physical, mental or moral development;	***Article 28a (1)(b)*** protect minors from content which may impair their physical, mental or moral development.	Article 28a (1)(a) protect minors from ***programmes, user-generated videos and audiovisual commercial communications*** which may impair their physical, mental or moral development;
	Article 28a (1)(b) protect all citizens from content containing incitement to violence or hatred directed against a group of persons or a member of such a group defined by reference to sex, race, colour, religion, descent or national or ethnic origin.	***Article 28a (1)(a)*** protect all citizens from content ***containing incitement to undermine human dignity, or*** content containing incitement to violence or hatred directed against ***a person or a group of persons*** defined by reference to ***nationality***, sex, race, colour, ethnic ***or social*** origin, ***genetic features, language***, religion ***or belief, political or any other opinion,***	Article 28a (1)(b) protect ***the general public from programmes, user-generated videos and audiovisual commercial communications*** containing incitement to violence or hatred directed ***against a group of persons or a member of such a group*** defined by reference to ***sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation;***

[245] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013.
[246] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0287:FIN.
[247] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0192&language=EN.
[248] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9691_2017_INIT&from=EN.

Current AVMSD 2010/13/EU[245]	Commission proposal 25 May 2016[246]	EP amendments 10 May 2017[247]	Council Gen. Approach 23 May 2017[248]
		membership of a national minority, property, birth, disability, age, gender, gender expression, gender identity, sexual orientation, residence status or health;	
			Article 28a (1)(ba) protect the general public from programmes, user-generated videos and audiovisual commercial communications containing the public provocation to commit a terrorist offence as set out in Article 5 of Directive (EU) 2017/541 on combating terrorism;
			1a. Member States shall ensure that video-sharing platform providers comply with the requirements set out in Article 9(1) with respect to audiovisual commercial communications that are marketed, sold and arranged by those video-sharing platform providers. Taking into account the limited control exercised by video sharing platforms over audiovisual commercial communication that are not marketed, sold and arranged by those video sharing platform providers, Member States shall ensure that the video sharing platform providers take appropriate measures to comply with the requirements set out in Article 9(1).
	Article 28a (2) What constitutes an appropriate measure for the purposes of paragraph 1 shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having created and/or uploaded the content as well as the public interest.	2. [See Article 28a (2a) below]	***For the purposes of paragraphs 1 and 1a, the appropriate measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having created and/or uploaded the content as well as the public interest. The measures shall be practicable and proportionate, taking into account the size of the video-***

Current AVMSD 2010/13/EU[245]	Commission proposal 25 May 2016[246]	EP amendments 10 May 2017[247]	Council Gen. Approach 23 May 2017[248]
			sharing platform service and the nature of the service that is provided.
	Those measures shall consist of, as appropriate:	Those measures shall consist of, as appropriate:	Such measures ***shall include***, as appropriate:
	Article 28a (2) a defining and applying in the terms and conditions of the video-sharing platform providers the concepts of incitement to violence or hatred as referred to in point (b) of paragraph 1 and of content which may impair the physical, mental or moral development of minors, in accordance with Articles 6 and 12 respectively;	defining and applying in the terms and conditions of the video-sharing platform providers the concepts of incitement to violence or hatred as referred to in point ***(a)*** of paragraph 1 and of content which may impair the physical, mental or moral development of minors, in accordance with ***Article 6(a) and (b) and Article 6a*** respectively. ***For the purposes of paragraph 1, Member States shall ensure that such measures based on terms and conditions are only permitted if national procedural rules provide the possibility for users to assert their rights before a court after learning of such measures;***	***including*** and applying, in the terms and conditions of the video-sharing platform ***services, the requirements not to incite to violence or hatred as referred to in point (b) of paragraph 1 and not to publicly provoke the commitment of terrorist offences as referred to in point (ba) of paragraph 1, in accordance with Article 6, as well as the concept of content which may impair the physical, mental or moral development of minors, in accordance with Article 12(1);***
			Article 28a (2)(aa) including and applying, in the terms and conditions of the video-sharing platform services, the requirements set out in Article 9(1) for audiovisual commercial communications that are not marketed, sold or arranged by the video-sharing platform providers;
	Article 28a (2) b establishing and operating mechanisms for users of video-sharing platforms to report or flag to the video-sharing platform provider concerned the content referred to in paragraph 1 stored on its platform;	establishing and operating ***transparent and user-friendly*** mechanisms for users of video-sharing platforms to report or flag to the video-sharing platform provider concerned the content referred to in paragraph 1 ***hosted*** on its platform;	establishing and operating mechanisms for users of video-sharing platforms to report or flag to the video-sharing platform provider concerned the content referred to in paragraph 1 ***stored*** on its platform;
		Article 28a (2) ba establishing and operating systems through which providers of video-sharing platforms explain to users of video-sharing platforms what effect has been given to the reporting and flagging referred to in point (b);	[DELETED]
	Article 28a (2) c		

Current AVMSD 2010/13/EU[245]	Commission proposal 25 May 2016[246]	EP amendments 10 May 2017[247]	Council Gen. Approach 23 May 2017[248]
	establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors;	establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical mental or moral development of minors; ***such systems shall not lead to any additional processing of personal data and shall be without prejudice to Article 8 of Regulation (EU) 2016/679;***	establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors;
	Article 28a (2) d establishing and operating systems allowing users of video-sharing platforms to rate the content referred to in paragraph 1;	establishing and operating ***easy-to-use*** systems allowing users of video-sharing platforms to rate the content referred to in paragraph 1;	establishing and operating systems allowing users of video-sharing platforms to rate the content referred to in paragraph 1;
	Article 28a (2) e providing for parental control systems with respect to content which may impair the physical, mental or moral development of minors;	providing for parental control systems ***that are under the control of the end-user and proportionate to the measures referred to in this paragraph and paragraph 3*** with respect to content which may impair the physical, mental or moral development of minors; ***the regulatory authorities and/or bodies shall provide the necessary guidelines to ensure that the measures taken respect the freedom of expression and include a requirement to inform users;***	providing for parental control systems with respect to content which may impair the physical, mental or moral development of minors;
	Article 28a (2) f establishing and operating systems through which providers of video-sharing platforms explain to users of video-sharing platforms what effect has been given to the reporting and flagging referred to in point (b).	establishing and operating ***transparent, easy-to-use and effective procedures for the handling and resolution of disputes between the video-sharing platform provider and its users in relation to the implementation of the measures referred to in points (b) to (f).***	establishing and operating systems through which providers of video-sharing platforms explain to users of video-sharing platforms what effect has been given to the reporting and flagging referred to in point (b);
			Article 28a (2) fa providing for effective media literacy measures and tools and raising users' awareness of these measures and tools.
	[See Article 28a (2) above]	Article 28a (2a) What constitutes an appropriate measure for the purposes of paragraph 1 shall be determined in light of the nature of the content in question, the harm it may	[See Article 28a (2) above]

Current AVMSD 2010/13/EU[245]	Commission proposal 25 May 2016[246]	EP amendments 10 May 2017[247]	Council Gen. Approach 23 May 2017[248]
		cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having uploaded the content as well as the public interest. ***Appropriate measures shall respect the freedom of expression and information, and media pluralism. The most harmful content shall be subject to the strictest measures. Such measures shall not lead to any ex-ante control measures or upload-filtering of content.***	
	Article 28a (3) For the purposes of the implementation of the measures referred to in paragraphs 1 and 2, Member States shall encourage co-regulation as provided for in Article 4(7).	For the purposes of the implementation of the measures referred to in paragraphs 1 and 2, ***Member States and the Commission*** shall encourage ***and facilitate self-regulation*** and co- regulation as provided for in Article 4(7) ***and (7a) ensuring that codes of conduct comply with the provisions of this Directive and fully respect the rights, freedoms and principles set out in the Charter, in particular Article 52 thereof. Member States shall ensure that video-sharing platform providers conduct and publish regular audits of their performance in accordance with the measures referred to in paragraph 1.***	For the purposes of the implementation of the measures referred to in ***paragraph 2***, ***Member States are encouraged to use*** co-regulation as provided for in ***Article 4a(1)***.
			Article 28a (3a) ***For the purposes of ensuring effective and consistent implementation of this Article, where necessary, the Commission shall, after consulting the Contact Committee, issue guidelines regarding the practical application of point (iii) of Article 1(aa).***
	Article 28a (4) Member States shall establish the necessary mechanisms to assess the appropriateness of the measures referred to in paragraphs 2 and 3 taken by	Member States shall establish the necessary mechanisms to assess ***and report on the delivery and effectiveness*** of the measures taken, taking into	Member States shall establish the necessary mechanisms to ***assess the appropriateness of the measures, referred to in paragraph 2 taken by video-***

Current AVMSD 2010/13/EU[245]	Commission proposal 25 May 2016[246]	EP amendments 10 May 2017[247]	Council Gen. Approach 23 May 2017[248]
	video-sharing platform providers. Member States shall entrust this task to the authorities designated in accordance with Article 30.	account their ***legality, transparency, necessity, effectiveness and proportionality***. Member States shall entrust this task to the authorities designated in accordance with Article 30. ***The regulatory authorities and/or bodies shall provide the necessary guidelines to ensure that the measures taken respect the freedom of expression, and include a requirement to inform users***.	***sharing platform providers. Member States shall entrust the assessment of those measures to the national regulatory authorities.***
	Article 28a (5) Member States shall not impose on video-sharing platform providers measures that are stricter than the measures referred to in paragraph 1 and 2. Member States shall not be precluded from imposing stricter measures with respect to illegal content. When adopting such measures, they shall respect the conditions set by applicable Union law, such as, where appropriate, those set in Articles 14 and 15 of Directive 2000/31/EC or Article 25 of Directive 2011/93/EU.	***Article 8 shall apply to video-sharing platform providers.*** " Article 8 Member States shall ensure that media service providers and video-sharing platform providers under their jurisdiction do not transmit cinematographic works outside periods agreed with the rights holders. "	***Member States may impose on video-sharing platform providers measures that are more detailed or stricter than the measures referred to in paragraph 2. When adopting such measures, Member States shall comply with the requirements set out by applicable Union law, such as those set in Articles 14 and 15 of Directive 2000/31/EC or Article 25 of Directive 2011/93/EU.***
		Article 28a (5a) ***Member States shall provide that sponsorship or audiovisual commercial communications that are marketed, sold, or arranged by video-sharing platform providers comply with the requirements of Articles 9 and 10.*** ***Without prejudice to Articles 14 and 15 of Directive 2000/31/EC, Member States shall provide that video-sharing platforms require users who upload content to declare whether such content contains advertisements, sponsored content or product placement.*** ***Member States shall require video-sharing platforms to provide that service recipients be clearly informed of declared or known content including advertisements,***	[DELETED]

Current AVMSD 2010/13/EU[245]	Commission proposal 25 May 2016[246]	EP amendments 10 May 2017[247]	Council Gen. Approach 23 May 2017[248]
		sponsored content or product placement.	
	Article 28a (6) Member States shall ensure that complaint and redress mechanisms are available for the settlement of disputes between users and video-sharing platform providers relating to the application of the appropriate measures referred to in paragraphs 1 and 2.	[DELETED]	Member States shall ensure that complaint and redress mechanisms are available for the settlement of disputes between users and video-sharing platform providers relating to ***the application of paragraphs 1 and 2.***
			Article 28a (6a) ***In addition to the measures referred to in paragraph 2, Member States shall encourage policies and schemes to develop media literacy skills.***
	Article 28a (7) The Commission and ERGA shall encourage video-sharing platform providers to exchange best practices on co-regulatory systems across the Union. Where appropriate, the Commission shall facilitate the development of Union codes of conduct.	The Commission and the ERGA shall encourage video-sharing platform providers to exchange best practices on ***self- regulatory and*** co-regulatory systems across the Union. Where appropriate, the Commission shall facilitate the development of Union codes of conduct.	***The Commission shall encourage video-sharing platform providers to exchange best practices on co-regulatory codes of conduct referred to in paragraph 3.***
	Article 28a (8) Video-sharing platform providers or, where applicable, the organisations representing those providers in this respect shall submit to the Commission draft Union codes of conduct and amendments to existing Union codes of conduct. The Commission may request ERGA to give an opinion on the drafts, amendments or extensions of those codes of conduct. The Commission may give appropriate publicity to those codes of conduct.	Video-sharing platform providers or, where applicable, the organisations representing those providers in this respect shall submit to the Commission draft Union codes of conduct and amendments to existing Union codes of conduct. The Commission may request ***the*** ERGA to give an opinion on the drafts, amendments or extensions of those codes of conduct. ***The Commission shall publish those codes in order to promote the exchange of best practices***.	***Member States and the Commission may foster self-regulation through Union codes of conduct referred to in Article 4a(2).***

Source: European Audiovisual Observatory elaboration on official EU documents.

Table 13. Revision process on provisions regarding the establishment of video-sharing platforms (Article 28b AVMSD)

Current AVMSD 2010/13/EU[249]	Commission proposal 25 May 2016[250]	EP amendments 10 May 2017[251]	Council Gen. Approach 23 May 2017[252]
			Article 28b (-1) ***For the purposes of this Directive, a video-sharing platform provider established on the territory of a Member State within the meaning of Article 3(1) of Directive 2000/31/EC shall be under the jurisdiction of that Member State.***
	Article 28b (1) Member States shall ensure that video-sharing platform providers which are not established on their territory, but which have either a parent company or a subsidiary that is established on their territory or which are part of a group and another entity of that group is established on their territory, are deemed to have been established on their territory for the purposes of Article 3(1) of Directive 2000/31/EEC.	No amendment	***A video-sharing platform provider which is not established on the territory of a Member State pursuant to paragraph -1 shall be deemed to be established on the territory of a Member State for the purposes of this Directive if that video-sharing platform provider:*** ***a) has a parent undertaking or a subsidiary undertaking that is established on the territory of that Member State; or*** ***b) is part of a group and another undertaking of that group is established on the territory of that Member State.*** ***For the purposes of this Article:*** ***a) "parent undertaking" means parent undertaking as defined in point 9 of Article 2 of Directive 2013/34/EU;*** ***b) "subsidiary undertaking" means subsidiary undertaking as defined in point 10 of Article 2 of Directive 2013/34/EU;*** ***c) "group" means a parent undertaking, all its subsidiary undertakings and all other undertakings which are part of the group.***

[249] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013.
[250] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0287:FIN.
[251] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0192&language=EN.
[252] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9691_2017_INIT&from=EN.

Current AVMSD 2010/13/EU[249]	Commission proposal 25 May 2016[250]	EP amendments 10 May 2017[251]	Council Gen. Approach 23 May 2017[252]
	For the purposes of applying the first subparagraph, where the parent company, the subsidiary or the other entity of the group are each established in different Member States, the provider shall be deemed to have been established in the Member State where its parent company is established or, in the absence of such an establishment in a Member State, where its subsidiary is established or, in the absence of such an establishment in a Member State, where the other entity of the group is established.	No amendment	***1a.*** For the purposes of applying ***paragraph 1***, where the parent ***undertaking***, the subsidiary ***undertaking*** or the other ***undertakings*** of the group are each established in different Member States, the ***video-sharing platform*** provider shall be deemed to ***be*** established in the Member State where its parent ***undertaking*** is established or, in the absence of such an establishment, in the Member State where its subsidiary ***undertaking*** is established or, in the absence of such an establishment, in the Member State where the other ***undertaking*** of the group is established.
	For the purposes of applying the second subparagraph, where there are several subsidiaries each of which are established in different Member States, or where there are several other entities of the group each of which are established in different Member States, the Member States concerned shall ensure that the provider designates in which of these Member States it shall be deemed to have been established.	No amendment	***1b.*** For the purposes of applying ***paragraph 1a***, where there are several ***subsidiary undertakings and each of them is established in a different Member State, the video-sharing platform provider shall be deemed to be established in the Member State where one of the subsidiary undertakings first began its activity, provided that it maintains a stable and effective link with the economy of that Member State. Where there are several other undertakings which are part of the group and each of them is established in a different Member State, the video-sharing platform provider shall be deemed to be established in the Member State where one of these undertakings first began its activity, provided that it maintains a stable and effective link with the economy of that Member State.***
			1c. For the purposes of this Directive, Articles 3, 14 and 15 of Directive 2000/31/EC shall apply to video-sharing platform providers deemed to be established in a Member State in accordance with

Current AVMSD 2010/13/EU[249]	Commission proposal 25 May 2016[250]	EP amendments 10 May 2017[251]	Council Gen. Approach 23 May 2017[252]
			paragraph 1.
	Article 28b (2) Member States shall communicate to the Commission a list of the video-sharing platform providers established on their territory and the criteria, set out in Article 3(1) of Directive 2000/31/EC and in paragraph 1, on which their jurisdiction is based. They shall update the list regularly. The Commission shall ensure that the competent independent regulatory authorities have access to this information.	Member States shall communicate to the Commission a list of the video-sharing platform providers established ***or deemed to be established*** on their territory ***in accordance with*** the criteria set out in paragraph 1, on which their jurisdiction is based. They shall update the list regularly. The Commission shall ensure that the competent independent regulatory authorities ***and/or bodies and the public have easy and effective*** access to this information.	Member States shall ***establish and maintain an up-to-date*** list of the video-sharing platform providers established ***or deemed to be established*** on their territory and ***indicate on which*** criteria, set out in ***paragraph -1 and 1***, their jurisdiction is based. ***Member States shall communicate this list, including any updates, to the Commission. In case of inconsistencies between the lists, the Commission shall contact the Member States concerned in order to find a solution***. The Commission shall ensure that the ***national regulatory authorities*** have access to this ***list. To the extent possible, the Commission shall make this information publicly available***.
		Article 28b (2a) ***Where, in applying paragraph 1, the Member States concerned do not agree on which Member State has jurisdiction, they shall bring the matter to the Commission's attention without undue delay. The Commission may request the ERGA to provide an opinion on the matter within 15 working days from the submission of the Commission's request.***	[DELETED]

Table 14. Revision process on provisions concerning the obligation to make certain information on the video-sharing platforms accessible to users (Article 28c AVMSD)

Current AVMSD 2010/13/EU[253]	Commission proposal 25 May 2016[254]	EP amendments 10 May 2017[255]	Council Gen. Approach 23 May 2017[256]
		Article 28c ***Member States shall ensure that a video-sharing platform provider under their jurisdiction make at least the following information easily, directly and permanently accessible to the user:*** ***(a) its name ;*** ***(b) the geographical address at which it is established;*** ***(c) the details, including its email address or website, which allow it to be contacted rapidly in a direct and effective manner;*** ***(d) the Member State having jurisdiction over it and the competent regulatory authorities and/or bodies or supervisory bodies.***	[DELETED]

[253] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013.
[254] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0287:FIN.
[255] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0192&language=EN.
[256] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9691_2017_INIT&from=EN.

A publication
of the European Audiovisual Observatory