cepStudy

# Liability for illegal content online

## Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a “Digital Services Act”

Anja Hoffmann & Alessandro Gasparotti

March 2020

## Key Issues

- The EU Commission announced that it will propose, in the fourth quarter of 2020, a Digital Services Act ("DSA") that will inter alia update liability rules for digital platforms, services, and products. An internal Commission note, leaked in summer 2019, outlines a number of amendments which the DSA might bring about to address specific problems of the existing regulatory framework.

- This cep**Study** focuses on the EU's approach to tackle illegal content online, and on digital service providers' liability for illegal content that users store on their platforms or otherwise disseminate via their services. It analyses the weaknesses of the current legal framework in this regard, and links them to possible regulatory measures that a future DSA might contain, according to the leaked Commission note.

- Currently, the E-Commerce Directive (ECD) protects certain providers of "information society services" – so-called intermediaries – by specific liability exemptions. The increased use of new types of digital services, such as cloud services, social media services or collaborative economy platforms inter alia raised questions on the providers' responsibilities with regard to the dissemination of illegal content via their platforms and on whether the existing rules are still up to date. The ECD has been complemented by sectoral legislation, soft law measures, and a growing body of jurisprudence from the Court of Justice of the European Union (CJEU). This has led to fragmentation and created a number of legal uncertainties, the most important of which are listed hereinafter (for the full list, see Chapter 4).

- For some providers of digital services, in particular "new services", it is unclear whether they fall under the ECD and/or may benefit from its liability exemptions. This leads to legal uncertainty regarding their liability for illegal content online. The DSA might therefore update the scope of and the liability provisions of the ECD, possibly transforming it into a regulation. Likewise, it might expand the ECD's liability exemptions explicitly to search engines and wifi hotspots, and clarify their application to "new" services such as collaborative economy services, cloud services, content delivery networks and domain name services.

- Other than the ECD, which does not apply to services supplied by service providers established only in a third country, the DSA might have an expanded territorial scope, and also apply to service providers established in third countries.

- Currently, only "passive providers" may profit from the ECD's liability exemptions, while providers exceeding the threshold of a certain "activity" risk to fall out of the scope of the liability exemption. The classification of an "active" or "passive" behaviour is questionable and complex; despite some guidelines set by CJEU in individual cases, national jurisprudence differs. The DSA might therefore replace the concept of the active or passive hosting provider with a more appropriate concept that instead focuses on whether the provider has "actual knowledge", "editorial functions", and a certain "degree of control", and thus better reflects the technical reality of today's services.

- Providers currently have little incentive to tackle illegal content proactively, as becoming aware of illegal content increases their liability risks. Illegal content is thus either not effectively tackled, or there is a risk of overblocking of lawful content. The DSA might thus include a binding "good Samaritan" provision, in order to encourage proactive measures to attack illegal content, and clarify the lack of liability as a result of such measures.

- The ECD and sectorial legislation oblige providers to remove or block content upon obtaining knowledge of its illegality, but there are no detailed rules on the applicable notice and action procedure. In order to prevent legal fragmentation, the DSA might create uniform, EU-wide binding "notice and action" rules for the removal of illegal content, which might be tailored to different types of providers and/or content.

- The ECD prohibits to impose on providers "general monitoring" obligations for illegal content online, while obligations to remove a specific infringing content – which imply a certain degree of "specific" monitoring – may be imposed on them, e.g. via injunctions. The DSA might consider certain provisions governing algorithms for automated filtering technologies – "where these are used" – while maintaining the prohibition of general monitoring obligations.

- Online platforms have become de-facto regulators with more and more powers, but without adequate and effective oversight. Public oversight on online platforms is split between different sectoral regulators, e.g. data protection authorities, competition authorities, regulators of electronic communication services, and consumer protection bodies. The DSA might create a new regulatory structure for online platforms, in order to improve public oversight and enforcement of rules, in particular for cross-border situations.

## Content

# 1 Introduction

The new EU Commission, led by President Ursula von der Leyen, has clearly identified creating a "Europe fit for the digital age" as a major priority. While this focus on digital policy will involve a wide range of initiatives, von der Leyen has inter alia specified in her Political Guidelines for the Commission that "a new Digital Services Act will upgrade our liability and safety rules for digital platforms, services and products, and complete our Digital Single Market".[1] This Digital Services Act has not been proposed yet, however, an internal Commission note[2] was leaked in summer 2019. This note is intended – as it states – to provide a basis for a discussion on "a potential new initiative […] to update the horizontal regulatory framework for all digital services in the single market, in particular for online platforms."[3] Part of this initiative might address questions concerning the liability of the providers of online services for illegal content such as illegal hate speech, terrorist content and material that infringes intellectual property rights, which they store on their platform or otherwise help to disseminate. In particular questions regarding the liability for the latter have repeatedly been at issue before the Court of Justice of the European Union (hereinafter: "CJEU"). These questions include, for instance, under what conditions providers of social media platforms like Facebook and other online platforms like eBay and Amazon can benefit from existing liability exemptions, and whether national courts may require e.g. providers like Facebook nevertheless to remove illegal content worldwide and even remove information whose content is not identical, but equivalent to the content of the information that was previously declared to be unlawful. These questions become more and more important as today's use of digital services, and in particular online platforms, is characterised by the creation of enormous amounts of user generated content. As a result, illegal and harmful content, which infringes on the rights of other persons, is increasingly being posted on the internet by third parties, who thereby abuse the services of digital service providers.

This cepStudy takes a closer look at whether and how the announced "Digital Services Act"[4] for the EU might harmonise the liability of digital service providers for illegal content disseminated through their online platforms or services, and the providers' respective removal duties.[5] For the purposes of this cepStudy, "illegal" content shall be understood as any information that is not in compliance with EU law or the law of a Member State. This may include, inter alia, illegal hate speech, child sexual abuse material, terrorist content, commercial scams and frauds and material that infringes intellectual property rights. In contrast, "harmful" content – i.e. content which is not necessarily illegal but could be offensive to some users, e.g. children, even if its publication is covered by freedom of speech and is thus not restricted –, as well as disinformation including "fake news" – which may hamper the ability of citizens to take informed decisions and thus pose a threat to democracy and fundamental rights of internet users – are not further discussed in this cepStudy.

---

1 Von der Leyen, POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2019-2024, available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf p. 13.

2 The paper was published i.a. on the website of netzpolitik.org, see https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf.

3 Internal Commission document (footnote 2), p. 1.

4 Another possible name for the "Digital Services Act" is "Digital Service Code", cf. Internal Commission document (Footnote 2), p. 4.

5 Other areas that might also be regulated by the envisaged "Digital Services Act" such as the regulation of online advertising and political advertising are not further discussed in this cepStudy. – like fake news –, and its content may change rapidly.

In order to understand the complex matter, Section 2 of this cepStudy first outlines the existing legal background with regard to providers' liability for illegal content and the problems arising from this status quo. Section 3 then describes how the Commission might consider addressing these problems in order to better tackle illegal content online. Section 4 finally summarises the main findings.

# 2 Legal background and weaknesses of the existing framework

This section describes the existing legal framework for the regulation of digital services. It starts with an overview of the fundamental rights which may be at stake when illegal content is disseminated via the internet (Section 2.1). Thereafter, it introduces the Directive on Electronic Commerce[6] (E-Commerce-Directive or EC-Directive, hereinafter: "ECD") of 2000 as the centrepiece of today's legal framework for digital services (see Section 2.2). Section 2.3 provides – as a consequence of the changed use of the internet in the past 20 years – a brief overview of new services that have emerged since the entry into force of the ECD and which the ECD does not therefore deal with explicitly. Thus, in the twenty years since entry into force of the ECD, the CJEU has issued a growing number of decisions on questions related to the ECD. A relevant selection of this case law will be presented in Section 2.4. Furthermore, in recent years, the ECD has been complemented by sectoral legislation that applies to specific services and products (see Section 2.5). Beyond this, some soft law initiatives have been launched (see Section 2.6). In addition, Section 2.7 illustrates two examples of national legislation which Member States are increasingly starting to adopt on important contemporary questions not yet regulated at EU level. Finally, an interim summary recapitulates the main characteristics of the existing legal framework and describes its possible consequences (Section 2.8).

## 2.1 Fundamental rights at stake

When regulating how to tackle illegal content online, the rights of different parties protected under the Union's legal order – notably those guaranteed in the Charter of Fundamental Rights of the European Union ("the Charter, hereinafter "CFR") – have to be taken into account. These fundamental rights include in particular[7]

- the internet users' freedom of expression and information, Art. 11 CFR, including the freedom to receive and impart information,
- the internet users' rights to respect for a person's private life, Art. 7 CFR, and to the protection of personal data, Art. 8 CFR,
- the service providers' freedom to conduct a business, Art. 16 CFR, including the freedom of contract of hosting providers,
- the right to (intellectual) property, Art. 17 para. 2 CFR,
- the rights of the child, Art. 24 CFR,
- the right to human dignity, Art. 1 CFR, and
- the right to non-discrimination, Art. 21 CFR
- the right to effective judicial protection of the users of the service concerned, Art. 47 CFR.

[6] 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').

[7] See also European Commission, recommendation of 1.3.2018 on measures to effectively tackle illegal content online, C(2018) 1177, Recital 13.

Those fundamental rights collide and must thus be carefully and fairly balanced, in particular when obliging service providers to remove or disable access to content which they store. For example, the removal of critical content may on the one hand protect the person whose rights are infringed by this content, while, on the other hand, it may restrict both the freedom of expression of the user who posted the content, as well as the freedom of information of other users.

Likewise, hosting providers play a central role in facilitating public debate and the distribution and reception of facts, opinions and ideas in accordance with the law, which has to be taken into account.[8]

## 2.2 The E-Commerce Directive [2000/31/EU]

The ECD sets out the basic legal framework for "information society services" in the EU and aims to "strike a balance" between the different interests at stake.[9] The ECD itself does not define or use the term "digital services", but relies on the definition of "information society services". An information society service is any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. [10] Mainly online services fall under this definition.

The ECD in general aims to remove obstacles to cross-border information society services in order to ensure the free movement of these services in the internal market, and to provide legal certainty for businesses and consumer confidence[11]. To achieve these objectives, the ECD harmonises certain national provisions.[12] Inter alia, the ECD establishes harmonised rules on

- transparency and information requirements for service providers,
- commercial communications, including advertising,
- electronic contracts and limitations of liability of intermediary service providers.

For the purpose of this cepStudy, which focuses on the liability of digital service providers for illegal content, the following key principles on which the ECD is based are relevant: the so-called home state control principle (see Section 2.2.1), the liability exemptions for certain intermediaries such as access and hosting providers (see Section 2.2.2), and the prohibition of general internet monitoring obligations (see Section 2.2.3).

### 2.2.1 The home state control principle

The ECD's internal market clause (Art. 3 para. 1 and recital 22 of the ECD) ensures that providers of information society services are in principle subject to the law of the Member State in which the service provider is established, and not the law of the Member States where the service is accessible (so-called "home state control principle" or "country of origin principle"). However, this does not apply to legal questions and areas of law which are expressly exempted from this principle, including copyright and industrial property rights.[13]

8 See also European Commission, l.c. (Footnote 7., Recital 1, 13).
9 See Recital 41 of the ECD.
10 See Art. 2 (a) ECD, Art. 1 (1) (b) Directive (EU) 2015/1535 (which has replaced Directive 98/48/EC).
11 Recital 5-7 ECD.
12 Art. 2 ECD.
13 See Art. 3 (3) and Annex of the ECD.

### 2.2.2 Liability exemptions for intermediaries

The conditions under which the liability of information society service providers arises are subject to the applicable national law. However, when it comes to liability for illegal content, a clear distinction must be made between the liability for own content and the liability for third party content.[14]

According to the ECD's basic rule, each provider of an information society service is responsible as a content provider under general law for its own information (content) which it makes available for use by others.[15]

In contrast, as regards the liability for third party content, the ECD[16] partly exempts three categories of information service providers that fulfil the role of "intermediaries" – who bring together or facilitate transactions between third parties on the Internet[17] – from secondary liability[18] for "information provided by a recipient of the service":

(1) **Access providers**[19] who merely transmit third-party information via a communication network, or provide access to a communication network ("mere conduit"), e.g. Vodafone or Deutsche Telekom;
(2) **Caching providers**[20] whose service consists of the automatic, intermediate and temporary storage of data – e.g. in the memory of a proxy server[21] – for the sole purpose of accelerating the onward transmission of the information (so-called "**caching**");
(3) **Hosting providers**[22] who host – i.e. store more than temporary – content authored by third parties, e.g. webhosting providers such as Amazon Web Services or Strato and social media providers such as Facebook.

One of the main reasons behind this so-called "safe harbour protection" of these three types of intermediaries is that they play an important role by enabling the free communication as well as economic and other activities over the internet. Therefore, the ECD seeks to restrict the situations in which intermediaries may be held liable pursuant to the applicable national law. It requires that the rules of national law on the liability of intermediaries must include the restrictions set out in the ECD.[23]

The exemptions are however limited to liability for damages, i.e. monetary liability, and only apply under certain conditions. In particular, hosting providers are – in simple terms – only exempt from liability for damages if

---

14 Grabitz-Hilf, Recht der Europäischen Union, 40. Auflage 2009, Sekundärrecht, A4 Art. 12 Vorbem. para. 2.
15 Grabitz-Hilf, l.c.
16 Art. 12-15 ECD.
17 European Parliament, Study, G. Sartor et. Al, Providers Liability: From the eCommerce Directive to the future IP/A/IMCO/2017-07, p.6 available under http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf.
18 Secondary liability is the liability for the actions of another party.
19 Art. 12 ECD.
20 Art. 13 ECD.
21 Grabitz/Hilf-Marly, Das Recht der EU, 40. Ed. 2009, Vorbem. A 4, para. 7. A proxy server stores copies of frequently accessed websites closer to users than the original server, and serves this information to them, see https://www.websense.com/content/support/library/web/v80/wcg_help/proxy2.aspx.
22 Art. 14 ECD.
23 CJEU, C-236/08, Google France, par. 107.

(1) they do not actually know that they are hosting "illegal activity or information", and are not aware of facts or circumstances from which the illegal nature of the information is apparent[24], and,

(2) in case they obtain such knowledge or awareness, they act "expeditiously" to remove the information, or to block access to this information[25] (so-called "notice and action" or "notice and take-down" requirement).

Hosting providers are thus exempt from liability for hosting third-party illegal content if they do not have "actual knowledge" of the illegal activity or information, and if, upon obtaining such knowledge or awareness, they expeditiously block or remove such content. The question when and how such actual knowledge or awareness is obtained must be evaluated on a case-by-case basis. The CJEU has provided some guidance on how "actual knowledge" or "awareness" is obtained in the case of intellectual property infringements. For the rest, the respective jurisprudence in the EU varies among Member States.[26] Likewise, the ECD does not further clarify when an intermediary may be said to have acted "expeditiously".

Beyond this, to benefit from the exemptions, the intermediary must not play an active, but a neutral, merely technical, automatic and passive role towards the specific information or activity hosted.[27] E.g., a hosting provider must not have knowledge or control over the stored information.[28] An access provider must neither have initiated the transmission, nor selected its receiver or the transmitted information, nor modified the latter.[29] Liability under the ECD thus depends on whether the intermediary is to be classified as an active or passive provider.

### 2.2.3 Prohibition of general internet monitoring obligations

The ECD further lays down the basic principle that EU Member States must not impose a *general* obligation on intermediaries to monitor the information they transmit or store, or to actively seek facts or circumstances indicating illegal activity.[30] As the ECD's liability exemptions only cover criminal liability and civil liability for damages, intermediaries may be ordered e.g. by a court to terminate or prevent infringements[31], and may thus be subject to injunctive relief. As a result, de facto monitoring obligations may be imposed on them so that no further infringement of rights occurs in the future. These monitoring obligations relate however to a specific infringement identified by a court and are thus not of a *general*, but a *specific* nature. The ECD does not exclude monitoring obligations "in a specific case" or orders issued by national authorities in accordance with national legislation.[32] Neither does it exclude Member States from specifying by national law "duties of care" to be applied by intermediaries

[24] Art. 14 (1) (a) ECD.
[25] Art. 14 (1) (b) ECD.
[26] See European Commission, Overview of the legal framework of notice-and-action procedures in Member States, SMART 2016/0039, Executive Summary, p. 2, for further details, available under: https://op.europa.eu/en/publication-detail/-/publication/c5fc48ac-2441-11e9-8d04-01aa75ed71a1/language-en/format-PDF/source-106371634.
[27] See Recital 42 ECD.
[28] CJEU, judgment of 12 July 2011, case C-324/09, L'Oréal/eBay, No. ECLI:EU:C:2011:474.
[29] Art. 12 (1) ECD.
[30] Art. 15 (1) ECD.
[31] Art. 12 (3), 13 (2), 14 (3) ECD.
[32] Recital 47 of the ECD.

in order to detect and prevent certain types of illegal activities.[33] It only precludes Member States from imposing internet monitoring obligations of a *general* nature on the protected intermediaries.

### 2.2.4 Regulatory loopholes in the E-Commerce Directive

In the view of the European Commission, the ECD's liability regime strikes a balance between the various interests that are at stake, in particular between the interests of intermediary services, the societal interest that illegal information is taken down quickly, and the protection of colliding fundamental rights.[34] However, there are also regulatory loopholes in the ECD which create legal uncertainty in applying its special liability rules.

**(1) Unclear liability of search engine operators and providers of hyperlinks**

As regards intermediaries that do not fall clearly under one of the categories of beneficiaries to which the ECD grants liability exemptions, their liability is unclear. This also affects services which were already common at the time when the ECD was drafted, in particular search engine operators such as Google and the providers of hyperlinks. Search engine operators and the providers of hyperlinks also fall within the ECD's definition of an information society service, but they cannot be classified as an access, caching or hosting provider that benefits from the ECD's liability exemptions because they do not meet the individual requirements of articles 12-14 of the ECD.[35]

**(2) No detailed "notice and action" procedure**

The ECD obliges intermediaries to remove information or to block access to it upon obtaining knowledge of its illegality, but it does not provide detailed rules for the applicable notice and action procedure. The ECD only foresees the possibility of introducing a notice and action procedure at EU level in the future.[36] Therefore, based on the ECD, the Member States have developed rules on notice and action procedures, which differ from each other.[37] In practice, a multitude of often very different procedures exist and it is difficult for both intermediaries and victims of illegal content to determine which one applies and in what way.[38]

**(3) No detailed regulation of the permissible scope of injunctions**

Furthermore, the ECD does not comprehensively regulate the permissible scope of injunctions, e.g. to cease and desist from making available a specific illegal content. On the one hand, the ECD states that general internet monitoring obligations must not be imposed on the protected intermediaries; on the other hand, specific monitoring obligations may be allowed. While these two obligations do not at first appear to be contradictory, the risk of being subject to an injunction followed by increased "specific"

---

33 Recital 48 of the ECD.

34 Commission Staff Working Document "Online services, including e-commerce, in the Single Market", SEC(2011) 1641 (final) accompanying COM (2011) 942, p. 24, available under https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011SC1641

35 Grabitz-Hilf, Recht der Europäischen Union, 40th Edition 2009, Sekundärrecht, A4 Art. 12 Vorbem. para. 8, 9.

36 Art. 21 (2) ECD.

37 European Commission, l.c. (Footnote 26), p.3.

38 Commission Staff Working Document "Online services, including e-commerce, in the Single Market", SEC(2011) 1641 (final) accompanying COM (2011) 942, p. 25, available under https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011SC1641.

monitoring obligations does harbour financial risks for intermediaries whom the ECD is generally designed to protect.

**(4) ECD not applicable to services supplied by providers established outside the EU**

Beyond this, the ECD does not apply to services supplied by service providers established only in a third country.[39] The ECD's home state control principle thus does not apply; rather, each Member State may define its policy with respect to those providers, provided that this policy conforms with international trade agreements.[40]

## 2.3 Technical and market developments since entry into force of the E-Commerce Directive

Since the ECD entered into force in 2000, the use of the internet and of digital services has evolved substantially.

Firstly, in parallel with the technical progress, the variety of services has increased. Many new types of digital services have emerged that were not envisaged when the ECD was adopted. They include inter alia

(1) cloud computing services – i.e. services offering the storing, processing and use of data on remotely located computers accessed over the internet[41] instead of on the user's own hardware – e.g. services offered by Google Drive, Microsoft OneDrive, Apple iCloud or Dropbox;
(2) content delivery networks – i.e. networks of geographically distributed servers that replicate, store (cache) and deliver websites and other web content, especially large media files, to internet users[42] – e.g. Amazon Web Services, Cloudflare or Microsoft Azure;
(3) social media services e.g. Facebook, Instagram, Twitter, YouTube, WhatsApp or TikTok;
(4) "collaborative economy" or "sharing economy" services – i.e. online platforms that provide an open marketplace for the temporary usage of goods or services, by connecting service providers who share assets, resources, time and/or skills with users of these services and thus facilitate transactions, e.g. renting of flats, car sharing, transport services; the services are often offered by private individuals on an occasional basis ("peer-to-peer"), but can also be provided by "professional" service providers[43] – e.g. AirBNB or Uber; such platforms often provide also a certain number of additional or ancillary services such as aftersale services;
(5) online advertising services e.g. Google Ads, Facebook Ads, Twitter Ads or Instagram Ads;

---

39 See Recital 58 of the ECD.
40 See communication COM(2001) 66 final, p. 6.
41 See definition of "Cloud Computing" of the European Commission in Communication "Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529, p. 2, available under http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF.
42 An internet user can thus access a copy of the content at a location that is geographically close to him. This allows faster content delivery than the traditional method of storing content on just one, central server, which all clients would access, and avoids bottlenecks near that server; see e.g. https://en.wikipedia.org/wiki/Content_delivery_network and https://www.globaldots.com/content-delivery-network-explained
43 See the definition of "collaborative economy" by the European Commission in Communication, COM(2016) 356, European agenda for the collaborative economy, p. 3, available under https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A356%3AFIN.

(6) digital services built on electronic contracts and distributed ledgers which have no central administrator or centralised data storage, e.g. blockchain technology including Bitcoin and other crypto currencies.

As these digital services were not known or common when the ECD was adopted, it is or was unclear whether they are generally covered by the ECD, and/or whether the providers of these new services may benefit from the liability exemptions for intermediaries. For services like collaborative economy services, the questions on liability for illegal content are only relevant to the extent they provide hosting services.[44]

Secondly, the habits of internet users and the role of the providers of digital services have changed considerably. For example, online platforms are today connecting an increasing number of users, information and services. Internet users are widely using social media to generate content and network with other users, gathering and sharing as much information as possible. Such platforms facilitate the propagation of content and thus also the exercise of related fundamental rights – in particular the internet users' freedom of expression and information. At the same time, they also facilitate the propagation of illegal content infringing e.g. intellectual property rights or other fundamental rights of individuals. Their role is even more important as these private companies have the power to include, exclude or rank content on their platform, which raises questions on their responsibility for the protection of fundamental rights. It is however unclear to what extent monitoring obligations to prevent (future) infringements can be legitimately imposed on such platforms by national courts.

These questions have thus repeatedly been the subject of litigation, up to the Court of Justice of the European Union. The following Section 2.4 presents the key findings of selected relevant CJEU rulings.

## 2.4 Selection of relevant case law

Regulatory loopholes in the ECD[45] and the emergence of new digital services have created a legal uncertainty on the general applicability of the ECD to providers of such services. This includes the question of whether and to what extent the providers of new services are covered by the ECD's liability exemptions – i.e. who falls under the definition of an "information society service" provider, or who fulfils the conditions of a hosting provider. The CJEU has therefore had to deal with quite a number of cases concerning these questions. The following table contains a brief summary of the key messages of selected relevant CJEU rulings.

**Tab. 1: Selection of relevant CJEU rulings**

| Case Reference and date | Parties | Case description | Main findings |
|---|---|---|---|
| **1. Jurisprudence on the definition of an information society service (general applicability of the ECD)** | | | |
| C-434/15<br><br>20-12-2017 | **Asociación Profesional Elite Taxi vs. Uber Spain** | Uber provides two types of services simultaneously:<br>(1) an intermediation service (online platform), on which non-professional drivers using their own vehicle can connect with passengers who wish to | **Uber's intermediation service does not fall within the scope of the ECD. It is an integral part of an overall service the main component of which is a transport service.**<br>An intermediation service like Uber's service fulfils, in principle, the criteria of an 'information society service' within the meaning of the ECD, but it is inherently linked with its urban transport services: without the App, drivers would not provide transport services and persons would not use |

[44] See COM(2016) 356 https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-356-EN-F1-1.PDF p. 7, 8.
[45] See above 2.2.4.

| | | | |
|---|---|---|---|
| | | make urban journeys through a Smartphone App; and<br>(2) urban transport services which it renders accessible through its software tools.<br>Spanish law requires an administrative license for providers of urban taxi services, which Uber does not hold. Is Uber's service merely a transport service or must it be considered an information society service? | their services. Uber influences the provision of the services by the drivers, e.g. it determines maximum fares and other conditions and exercises quality control. Therefore, its intermediation service forms an integral part of an overall service the main component of which is a transport service. It must thus be classified as 'a service in the field of transport' within the meaning of Article 58(1) TFEU which is excluded from the scope of Article 56 TFEU, the Services Directive 2006/123 and the ECD. |
| C-390/18<br><br>19-12-2019 | **Airbnb Ireland** | Airbnb provides<br>(1) an intermediation service (online platform) on which it connects – for remuneration – potential guests with professional or non-professional hosting providers offering short-term accommodation services; and<br>(2) a certain number of services ancillary to that intermediation service.<br>Does this service have to be considered an information society service? | **Airbnb's intermediation service qualifies as an information society service and thus falls within the scope of the ECD. It is not an integral part of an overall service the main component of which is an accommodation service.**<br>An intermediation service like the one of Airbnb must be classified as an "information society service". AirBNB's intermediation service does not form an integral part of an overall service whose main component is an accommodation service. Its intermediation service relates to subsequent accommodation services, but<br>- it is distinct from the subsequent accommodation service;<br>- it is separable from the property transaction, and not merely ancillary to the provision of an accommodation service;<br>- it is in no way indispensable to the provision of accommodation services;<br>- the nature of the links between those services does not justify a deviation from this classification;<br>- unlike Uber[46], Airbnb does not exercise a decisive influence over the conditions for the provision of the accommodation services; in particular, it does not determine the rental price charged, nor does it select the hosting providers or the accommodation put up for rent on its platform. |
| **2. Jurisprudence on the applicability and preconditions for the liability exemptions of the ECD** | | | |
| C-236/08<br>C-237/08<br>C-238/08<br><br>23-03-2010 | **Google France SARL vs. Louis Vuitton et al.** | Google operates<br>(1) a search engine with a classic search function;<br>(2) a paid referencing service called 'AdWords': advertisers may reserve keywords to obtain the placing of an advertising link to their website when an internet user enters this word as a request in the search engine. That advertising link appears under the heading 'sponsored links' separately from the "natural" search results. Advertisers were not only able to reserve keywords which corresponded to Vuitton's trademarks, but also to combine those keywords with expressions such as 'imitation' and 'copy'.<br>Can a provider like Google be exempted from liability according to Art. 14 of the ECD? | **An internet referencing service (like Google's) fulfils all elements of the definition of an information society service.**<br>**However, its provider can only be exempted from liability according to Art. 14 of the ECD (hosting provider) if – what the national court must assess – it has played a neutral and not an active role which gives it knowledge of, or control over, the data stored.**<br>If it acted neutrally, 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 – it is not liable for the data which it has stored at the request of an advertiser, unless it<br>- obtained knowledge of the unlawful nature of that data or of that advertiser's activities, and<br>-failed to act expeditiously to remove or to disable access to this data.<br>The following mere facts do not justify the view that Google has knowledge of, or control over, the data entered into its system by advertisers and stored on its server, and thus do not deprive Google of the exemptions from liability provided:<br>-the referencing service is paid, Google sets the payment terms and provides general information to its clients |

[46] See the judgments listed above.

| | | | |
|---|---|---|---|
| | | | -the mere concordance between the selected keyword and the search term entered by an internet user.<br>However, Google's role in the drafting of the commercial message which accompanies the advertising link, or in the establishment or selection of keywords may be relevant. |
| C-324/09<br><br>12-07-2011 | **L'Oréal vs. eBay** | EBay operates an online marketplace.<br>Is eBay liable for sales of goods which infringe trademark law, committed by its customer-sellers on its platform?<br>Can a provider like eBay – who stores the offers for sale on its server – be regarded as a hosting provider which is exempt from liability according to Art. 14 ECD?<br><br>Can a provider like eBay be ordered in an injunction to take measures to prevent future infringements of intellectual property rights, and if so, what measures might that be? | **The operator of an online marketplace (like eBay) plays an „active role"– which allows him to have knowledge or control of the data stored – inter alia when he assists his customers to promote or optimise the presentation of their sales offers.**<br>The national Court must decide whether eBay played such a role.<br>**Even if the operator has not played an active role, it cannot rely on the liability exemption in Art. 14 ECD if**<br>- **it becomes – whether through notification or as the result of an investigation undertaken on its own initiative – aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the sales offers in question were unlawful, and**<br>-**failed to act expeditiously to remove or to disable access to them.**<br>**Providers of online marketplaces may be ordered in injunctions to take measures to prevent future infringements of intellectual property rights of that kind, e.g. by the same seller in respect of the same trademark, provided that**<br>- **such injunction is effective and proportionate,**<br>-**the measures strike a fair balance between the various rights and interests in question and are not excessively costly;**<br>-**the measures do not involve active monitoring of all the data of each of the provider's customers in order to prevent any future infringement of intellectual property rights via that provider's website.**<br>**(Art. 15 ECD, Article 3 of Directive 2004/48)** |
| C-70/10<br>24-11-2011 | **Scarlet Extended vs. SABAM** | Scarlet, an internet service provider, offered its customers internet access (without further services such as downloading or file sharing). Some of its customers downloaded copyright-protected musical works via peer-to-peer file-sharing networks without an authorisation and without paying royalties. SABAM, the management company representing the authors of the affected works, sued Scarlet in order to require it to take technical measures (e.g. install a filtering system) to stop such copyright infringements committed by its customers through the use of its services.<br>Can an internet service provider like Scarlet be ordered in an injunction to install such filtering system? | No general obligation to monitor stored information:<br>**National courts must not require an internet service provider – in an injunction – to install a system for filtering all electronic communications passing via its services –** in particular those involving the use of peer-to-peer software–<br>- **which applies indiscriminately to all its customers;**<br>- **as a preventive measure;**<br>- **exclusively at its expense; and**<br>- **for an unlimited period,**<br>**which is capable of identifying on that provider's network the movement of electronic files containing a copyright-protected work, with a view to blocking the transfer of such files** (the sharing of which infringes copyright).<br>**This duty would oblige the provider to carry out general monitoring, which is prohibited by Article 15 ECD**, as it would have to actively monitor all data relating to each of its customers in order to prevent any future infringement of intellectual-property rights.<br>The ECD – read together with directives 2001/29, 2004/48, 95/46 and 2002/58 and construed in the light of the requirements stemming from the protection of the applicable fundamental rights – precludes this. |
| C-360/10<br><br>16-02-2012 | **SABAM vs. Netlog NV** | Netlog runs an online social networking platform on which its users can acquire and fill a personal space ("profile").<br>SABAM, the management company representing the authors of the | **The owner of an online social networking platform – such as Netlog – stores information provided by its users on its servers and is thus a hosting provider under Art. 14 ECD.**<br>No general obligation to monitor stored information: |

| | | | |
|---|---|---|---|
| | | affected works, alleges that Netlog users make works from SABAM's repertoire available to the public so that other users can access them without consent and fee, and asked them to give an undertaking to cease and desist. | **National courts must not require a hosting provider – in an injunction – to install a system for filtering all information stored on its servers by its users,**<br>**-which applies indiscriminately to all of those users;**<br>**-as a preventive measure;**<br>**-exclusively at its expense, and**<br>**-for an unlimited period,**<br>**which is capable of identifying electronic files containing copyright-protected works, with a view to preventing those works from being made available to the public in breach of copyright**.<br>The ECD – read together with directives 2001/29 and 2004/48 and construed in the light of the requirements stemming from the protection of the applicable fundamental rights – precludes this. |
| C-484/14 | **Mr. McFadden vs. Sony Music Entertainment** | Mr. McFadden operated in the vicinity of his business a wireless local area network (WLAN) to which he offered potential clients a free and anonymous access. A third party used this WLAN in order to make a phonogram produced by Sony Music available to the general public without authorisation.<br>Is a wifi provider like Mr. McFadden liable for this copyright infringement?<br>Can it be obliged by means of an injunction to prevent third parties from making a particular copyright-protected work or parts thereof available to the public? | **The provision of a wireless local area network (WLAN) – like the one operated by Mr. McFadden – constitutes an "information society service" within the meaning of Article 12 ECD if the provider runs the WLAN for the purposes of advertising his goods or services.** This means operators of such open WLANs are equal to access providers.<br>**Article 12 ECD does not exempt access providers from claims for injunctive relief by a national authority or court against the continuation of that infringement and for the payment of related costs**. It only exempts them from damages claims and from the reimbursement of the costs in relation to these claims.<br>**National courts can also issue an injunction against communication network access providers in order to prevent third parties from making a particular copyright-protected work or parts thereof available to the public from an online (peer-to-peer) exchange platform via its network, if the provider can choose the technical measures he will use to comply with the injunction**. This applies even if his choice is limited to password-protecting the internet connection, provided that users cannot act anonymously, but must reveal their identity in order to obtain the password.<br>This results from Art 12 ECD read in conjunction with the requirements deriving from the protection of fundamental rights and the rules laid down in Directives 2001/29 and 2004/48. |
| C-18/18<br><br>03-10-2019 | **Glawischnig-Piesczek vs. Facebook Ireland Ltd.** | Facebook Ireland operates a global social media platform on which a user shared – on his personal Facebook page but accessible for any Facebook user – an article and a comment which was illegal, as it insulted and defamed the Austrian politician Mrs. Glawischnig-Piesczek.<br>Can the injunction order, requiring a host provider like Facebook to cease and desist from publishing and/or disseminating specific illegal information, also be extended to the following statements, of which the provider is not aware:<br>- statements with identical wording, and<br>- statements with equivalent content?<br>Or does Art. 15 ECD preclude this?<br>Must the provider's obligation be limited to information posted by the | Removal of identical information:<br>**Art. 15 ECD does not preclude a national court from obliging a hosting provider like Facebook to remove and/or block access to stored information with content which is identical to the information which was previously declared to be unlawful, irrespective of who requested the storage of that information** (i.e. the user who originally posted the illegal information, or a third person).<br>Removal of equivalent information:<br>**Art. 15 ECD does not preclude a national court from obliging a hosting provider like Facebook to remove and/or block access to stored information with content which is equivalent to the information which was previously declared to be unlawful, subject to the following conditions: Providers like Facebook may also be required to monitor and search for equivalent information with slightly different wording, but only**<br>- **limited to information which contains the same specific elements as the originally illegal information (which are properly identified in the injunction) and thus conveys an "essentially unchanged" message,** |

| | | | |
|---|---|---|---|
| | | same user, or can it also be extended to information posted by other users?<br>Can the provider only be ordered to remove the information in the respective Member State, or can he be ordered to remove it worldwide? | - **provided that the differences in the wording of the equivalent content are sufficiently minor that the hosting provider can use automated search tools and technologies and would not have to carry out an independent assessment of that content.**<br>Such a duty would not impose on the provider a general monitoring duty within the meaning of Art. 15 ECD, but only a monitoring duty 'in a specific case'. Such a specific case may refer to specific information stored by a host provider, the content of which was declared by a competent court to be illegal.<br>Removal of information worldwide:<br>**The ECD does not preclude a national court from ordering a hosting provider to remove information or to block access to that information worldwide.** Member States must however ensure that the measures which they adopt, and which produce effects worldwide, take due account of the relevant international law. |
| C-567/18 | **Amazon Vs. Coty Germany** | Amazon operates a marketplace on which it offers third parties the possibility of offering goods on its website. Third-party suppliers may participate in the "Shipping by Amazon" programme, under which Amazon stores the goods in its logistics centres, ships the goods to the purchaser and provides additional services to the supplier.<br>"Davidoff" perfumes, which have not been put on the market with the consent of the trademark proprietor, are being offered via the Amazon marketplace and stored and shipped by Amazon.<br>Coty Germany, which holds a licence to the mark "Davidoff", sued Amazon, arguing that not only is the supplier of those perfumes committing a trademark infringement, but also Amazon, if the latter stores and dispatches the goods for the supplier.<br>Does a provider like Amazon – which stores goods that infringe trademark rights for a third party – possess these goods "for the purpose of offering or putting them into circulation", and thus itself commit trademark infringements, even if the provider has no knowledge of this violation and even if the supplier alone wishes to offer the goods? | Opinion of Advocate General Campos Sánchez-Bordona of 28/11/2019:<br>**If a person (here: Amazon) is actively involved in the distribution of trademark infringing goods within the framework of a programme like the "Shipping through Amazon" programme, which the seller has joined, it can be assumed to be storing the goods for the purpose of offering them on the market.**<br>**Undertakings who are substantially involved in the marketing of the product through the said programme must take special care with regard to the control of the legality of the goods traded.**<br>The mere fact that such undertaking is unaware of the trademark infringement does not exempt it from liability, provided that it could reasonably be expected to provide the means necessary to detect that violation.<br>In order to strike an appropriate balance between the protection of trademark rights and the prevention of barriers to legitimate trade, it is preferable to make a distinction between intermediaries on the basis of the nature of the services provided to the direct author of the trademark infringement.<br>• In contrast, a mere warehouse keeper, who performs only ancillary tasks, would be exempted from liability if it had no knowledge of the unlawfulness of the putting of the goods on the market by a seller without respecting the right of the trademark proprietor, and could not reasonably have had such knowledge. |
| **Other jurisprudence on questions of internet providers' liability** | | | |
| C-160/15<br><br>08-09-2016 | **GS Media BV vs. Sanoma Media,** | GS Media operated a website in the Netherlands on which it posted a news article which – by means of a hyperlink – referred to an Australian homepage, on which photos of Mme Dekker that were to be published in the Playboy magazine were | No general liability for hyperlinks:<br>A person who posts on its website a hyperlink to another website on which a copyright-protected work is published without the author's consent does not "communicate" this work to the public if that person<br>- does not seek financial gain and |

| | | | |
|---|---|---|---|
| | **Playboy Enterprises., Mme Dekker** | made available for download without authorisation from Sanoma, the author and publisher of that magazine.<br>Is GS Media liable for hyperlinks which allow access to previously unpublished copyrighted material? Does the provision of the link constitute a communication of the photos to the public, so that GS Media – by its own action – commits a copyright infringement? | - acts without knowledge that those works have been published illegally.<br>In contrast, **if a hyperlink is provided for profit, there is a rebuttable presumption that the hyperlink was posted with the full knowledge of the illegality of the publication on the other website. In this case, the act of posting a hyperlink to a work which was illegally placed on the internet constitutes a "communication to the public" within the meaning of Article 3 of Directive 2001/29**, unless the rebuttable presumption is rebutted. It can be expected that the person who posts such a link for profit carries out the necessary checks to ensure that the work concerned is not illegally published on the website to which the hyperlink leads. |

## 2.5 Sector-specific legislation

While the ECD as such applies horizontally to all information society services, independent of the sector, and its liability rules apply to any kind of illegal or infringing content, the Commission has in recent years taken a sector and problem-specific approach to regulate the tackling of particular types of illegal content on the internet. The most important pieces of such legislation are listed hereinafter. They build upon the ECD and leave its general liability principles unaffected but oblige the respective providers to take specific measures in order to tackle illegal content on their platforms.

### 2.5.1 Directive 2010/13/EU on the provision of audiovisual media services

Directive 2010/13/EU on the provision of audiovisual media services (hereinafter: "AVMSD"), updated by the recent amending Directive (EU) 2018/1808 [cf. cep**PolicyBrief** 2016-23], provides for a minimum harmonisation of national rules which govern the provision of audiovisual media services[47] (including Pay-TV, live-streaming and video-on-demand services) and video-sharing platform services[48] (e.g. YouTube). Video sharing platforms store and provide, e.g. via the internet, programmes or user-generated videos to the general public in order to inform, entertain or educate people. The provider of the platform has no "editorial responsibility" for the content, but is responsible for the organisation of the programmes and videos.[49] Social networks, like Facebook, fall under the AVMSD if the provision of broadcasts and videos is an essential function of that network.[50] In addition, the AVMSD also contains rules for the use of audiovisual commercial communications which accompany a video or programme (e.g. advertising) or are included in it (e.g. product placement).[51]

[47] "Audiovisual media service" means: (i) a service as defined by Articles 56 and 57 TFEU which is under the editorial responsibility of a media service provider and the principal purpose of which is the provision of programs, in order to inform, entertain or educate, to the general public by electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC. Such an audiovisual media service is either a television broadcast (…) or an on-demand audiovisual media service (…) and (ii) audiovisual commercial communication, see Art. 1 (1) (a) Directive 2010/13/EU.

[48] "Video-sharing platform service" means a service as defined by Articles 56 and 57 TFEU, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programs, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing, see Art. 1 (1) (b) Directive (EU) 2018/1808.

[49] Art. 1 No. 1 (aa) AVMSD.

[50] Ukrow/Ress, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, June 2019, Art. 167 No. 214.

[51] Art. 1 (a) (ii) and (h), Art. 9 et seq. AVMSD.

Comparable to the ECD's home state control principle, Member States are responsible for ensuring that audiovisual media services transmitted by service providers which are under their jurisdiction – e.g. because the provider is established or deemed to be established on their territory – comply with the respective rules in that Member State.[52] The ECD's liability exemptions also generally apply to audiovisual media[53] and video sharing services.[54] Nevertheless, the AVMSD obliges Member States to take necessary measures to ensure that audiovisual media services do not contain incitements to violence or hatred or public provocations to commit a terrorist offence.[55] Likewise, Member States must – "without prejudice" to the liability exemptions in the ECD – oblige video-sharing platform providers inter alia to take "appropriate measures", e.g. the protection of minors and the general public from content which contains such incitements or the dissemination of which is a criminal offence (e.g. terrorism or child pornography).[56]

### 2.5.2 The InfoSoc Directive 2001/29/EU and the Copyright Directive (EU) 2019/790

EU copyright legislation consists of eleven directives and two regulations[57] which harmonise the essential rights of authors and of performers, producers and broadcasters, and includes in particular Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (the so-called "InfoSoc-Directive") and the EU Database Directive 96/9/EC. Art. 8 (3) of the InfoSoc Directive, Member States must ensure that rightsholders may apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

The InfoSoc Directive and the EU Database Directive have recently been amended by Directive (EU) 2019/790[58] which was finally adopted in spring 2019 after long and intensive discussions [hereinafter "Copyright Directive 2019", cf. cep**Policy Brief** No. 2017-04]. This directive – which must be implemented by 7 June 2021 – reforms EU copyright law and adapts it to the digital and cross-border environment, leaving Art. 8 (3) of the InfoSoc Directive unaffected. The Copyright Directive 2019 contains, inter alia, new rules relevant to the liability of online services: inter alia, Member States must provide that an "online content-sharing service provider"[59] – who enables public access to a work uploaded by a user – itself performs an act of "communicating or making available the work to the public", for which it is liable under copyright law unless it is authorised to do so.[60] This means that online content-sharing service providers can now be held responsible for copyright infringements caused by the actions of their users, as their activity to enable public access to such infringing works is seen as their own (and thus primary) infringement. The Directive expressly states that the limitation of liability for hosting providers under the ECD[61] does not apply in this case.[62] This is consistent, as if online content-sharing

52 See Art. 2 AVMSD for audiovisual media services and Art. 28a AVMSD for video-sharing platform services.
53 Art. 4 (7) AVMSD.
54 Expressly Art. 28 (5) AVMSD for video-sharing platform providers „deemed to be established in a Member State".
55 Art. 6 (1) and (2) AVMSD.
56 Art. 28b AVMSD.
57 For further details cf. the Website of the European Commission, https://ec.europa.eu/digital-single-market/en/eu-copyright-legislation.
58 Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, available under https://eur-lex.europa.eu/eli/dir/2019/790/oj.
59 An "online content-sharing service provider" is a provider of an information society service of which the main purpose is to store and give the public access to a large amount of copyright-protected works uploaded by its users, which it organises and promotes for profit-making purposes, see Art. 2 (6) Directive (EU) 2019/790.
60 Art. 17 (2) Directive (EU) 2019/790.
61 Art. 14 ECD.
62 Art. 17 (3) Directive (EU) 2019/790.

service providers are deemed to be committing a primary copyright infringement, they can no longer invoke the exemption applicable to secondary liability.

Therefore, the directive obliges online content-sharing service providers to obtain permission from rightsholders in order to make works uploaded by the users on their platforms available to the public, for example through a licensing agreement.[63] If a provider does not conclude a license, it can only be exempted from liability if it proves that it has fulfilled all requirements of a new liability exemption regime:

(1) The provider must have made "best efforts" to obtain a license;
(2) The provider must have made "best efforts" to ensure the unavailability of specific works for which rightsholders have provided information;
(3) Upon receiving a substantiated notice from rightsholders, the provider must have acted expeditiously to remove the notified works from its website or disable access to them;
(4) Upon receiving a substantiated notice from rightsholders, the provider must also have made "best efforts" to prevent the future upload of the notified works.[64]

For new and small providers – whose services have been publicly available for less than three years, and which have an annual turnover below EUR 10 million – the rules on qualifying for an exemption from liability are less strict[65]: these providers are not liable if they prove to have fulfilled conditions (1) and (3), unless "the average number of monthly unique visitors" of these service providers exceeds 5 million. In the latter case, they also have to fulfil condition 4.

These new provisions on liability have been broadly criticised as threatening the freedom of expression and information on the internet. There is thought to be a risk that platforms who do not conclude licenses will only be able to fulfil the requirements by using technical solutions such as upload filters. These critics say that the use of such software-based filters can also lead to the unintentional blocking of legitimate content, as these filters do not recognise e.g. parody, caricature, criticism or quotations (so-called "overblocking"). However, the Directive provides that the cooperation between providers and rightsholders shall not prevent the availability of works which do not infringe copyright and related rights[66], and that – in case of unjustified blocking or other disputes – users may use complaint and redress mechanisms which the Member States must put in place.[67]

### 2.5.3 The Enforcement Directive 2004/48/EC

Similar to the InfoSoc Directive, the so-called "Enforcement Directive" 2004/48/EC[68] obliges Member States to provide for remedies necessary to ensure the enforcement of intellectual property rights such as trademark rights and other industrial property rights.[69] It also requires Member States to ensure that rightsholders may apply for an injunction against intermediaries whose services are being used by a third party to infringe an intellectual property right.[70]

63 Art. 17 (3) Directive (EU) 2019/790.
64 Art. 17 (4) and (5) Directive (EU) 2019/790.
65 Art. 17 (6) Directive (EU) 2019/790.
66 Art. 17 (7) Directive (EU) 2019/790.
67 Art. 17 (9) Directive (EU) 2019/790.
68 Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights.
69 Art. 3 Directive 2004/48/EC.
70 Art. 11 Directive 2004/48/EC.

### 2.5.4 Directive (EU) 2017/541 on Combating Terrorism and Proposed Regulation COM(2018) 640 on preventing the dissemination of terrorist content

As regards incitements to terrorism, Directive (EU) 2017/541 on Combating Terrorism requires Member States to ensure that the making available of a message to the public with an intentional incitement to commit a terrorist offence is punishable as a criminal offence.[71] Beyond this, Member States must "take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence".[72] If the removal is not feasible, Member States may take measures to block access to such content towards the internet users within their territory. They must also take care that there are transparent procedures for removal and blocking and adequate safeguards including the possibility of judicial redress.

In September 2018 the Commission proposed Regulation COM(2018) 640 on preventing the dissemination of terrorist content online, which is "closely aligned" with the aforementioned Directive. The Regulation aims to inscribe into EU law the existing non-binding measures[73] against the dissemination of terrorist content online. The proposed Regulation should not affect the application of the ECD, i.e. hosting providers[74] remain exempt from liability when taking measures or proactive measures in compliance with the proposed Regulation.[75] One of the innovations of the proposed Regulation is that once a competent authority[76] issues a decision requiring a hosting provider to remove terrorist content (or disable access to it), such removal must happen "within one hour from the receipt of the removal order".[77] Hosting providers are requested to take proactive measures to protect their services against the dissemination of terrorist content. Such measures must be effective and proportionate, taking into account the risk and level of exposure to terrorist content, and the fundamental rights of the users.[78] Where hosting providers use automated tools to prevent the dissemination of terrorist content, they must provide effective and appropriate safeguards, including human oversight[79], to ensure that the decisions made are accurate.[80] Hosting providers must reinstate the content without undue delay where the removal or disabling of access was unjustified, and inform the complainant about the outcome of the examination.[81] The proposed Regulation also foresees penalties in case of noncompliance: "Member States shall ensure that a systemic failure to comply with obligations to remove content within one hour from its notification is subject to financial penalties of up to 4% of the hosting provider's global turnover of the last business year".[82] However, the proposed Regulation only stipulates notice and action obligations following a notice from competent authorities and not for illegal content flagged by users.

---

71 Art. 5 Directive (EU) 2017/541 on Combating Terrorism.
72 Art. 21 Directive (EU) 2017/541 on Combating Terrorism.
73 See also Communication COM(2017) 555 "Tackling Illegal Content Online, containing guidelines on detection and removal of illegal content online, i.a. terrorist propaganda, and Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online, which includes a list of voluntary measures to flag and process illegal content online (see below Section 2.6.2).
74 Art.14 ECD.
75 Recital 5 of the proposed Regulation COM(2018) 640.
76 Designated by Member States as per Art.17 of the proposed Regulation COM(2018) 640.
77 Art.4 (1) and (2) of the proposed Regulation COM(2018) 640.
78 Art.6 (1) of the proposed Regulation COM(2018) 640.
79 Art.9 (2) of the proposed Regulation COM(2018) 640.
80 Art.9 (1) of the proposed Regulation COM(2018) 640.
81 Art.10 (2) of the proposed Regulation COM(2018) 640.
82 Art.18 (4) of the proposed Regulation COM(2018) 640.

The proposed Regulation has been endorsed by the Council, whereas the Parliament voted a number of amendments[83] on 17 April 2019. The text adopted by the European Parliament includes i.a. the following changes:

(1) It narrows the definition of hosting provider to "services provided to the public at the application layer". Cloud providers and electronic communications services (e.g. messaging applications) are explicitly excluded from the scope of the Regulation.
(2) It defines "competent authority" as a single designated judicial authority or functionally independent administrative authority in the Member State.
(3) It deletes the provision establishing a right for the competent authority to refer content to a service provider for the evaluation and deletion based on the provider's own terms and conditions.
(4) It reaffirms the prohibition of general monitoring, cancels provisions that could force providers to implement proactive measures such as automated tools preventing the re-upload of content which has previously been removed.

Informal negotiations between Commission, Council and Parliament (so called "trialogue") are currently underway in order to find a compromise on the final legislative text.

### 2.5.5 Regulation (EU) 2019/1148 on marketing and use of explosive precursors

Regulation (EU) 2019/1148[84] repeals Regulation (EU) No. 98/2013, which established harmonised rules concerning the making available, introduction, possession and use of substances or mixtures that could be misused for the illicit manufacture of explosives. Regulation (EU) No. 98/2013 was replaced to address a few weaknesses recognised in a report in 2017.[85] The problems related to substantial variations in licensing regimes across countries for the legal purchase of such substances or mixtures, and to the monitoring of online purchase, imports and intra-EU movements. The report suggested that national authorities should have greater capacity for monitoring the selling of such products. Regarding the liability of online intermediaries, the Regulation states that online marketplaces "should be subject to the same detection and reporting obligations as economic operators, although procedures to detect suspicious transactions should be adapted to the online environment".[86] This means that online intermediaries, like economic operators, need to report suspicious transactions to a national contact point of the Member State in which they are based within 24 hours of considering that such transaction is suspicious.[87] The Regulation is considered by the legislator to be in line with Art. 14-15 of the ECD, in that the detection and reporting obligations for online marketplaces are *specific* obligations with respect to the detection and reporting of suspicious transactions but should not amount to a *general* monitoring obligation.[88] Online marketplaces must have in place appropriate, reasonable and proportionate procedures to detect suspicious transactions[89], but they should not be held liable for transactions that they have not detected despite the use of such appropriate procedures.

---

83 https://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_EN.html .
84 Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors , amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013.
85 COM(2017) 103 Report from the Commission on the application of, and delegation of power under, Regulation (EU) 98/2013 on the marketing and use of explosives precursors.
86 Recital 15 of Regulation (EU) 2019/1148.
87 Art. 9 (4) Regulation (EU) 2019/1148.
88 Recital 16 of Regulation (EU) 2019/1148.
89 Art. 9 (2) Regulation (EU) 2019/1148.

### 2.5.6 Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography

The Directive[90] replaces Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography. Such legislation approximates Member States' legislation to criminalise the most serious forms of sexual abuse towards children. Among the various provisions, Art. 25 describes "measures against websites containing or disseminating child pornography". These measures are deemed to be in line with the liability exemption provided for in the ECD.[91] The Directive requires Member States to take the necessary measures to ensure the prompt removal of webpages disseminating child pornography hosted in their country, and to endeavour to obtain the removal of such pages when hosted outside their territory.[92] The Directive also states that Member States "may take measures to block access to web pages containing or disseminating child pornography within their territory".[93] These measures must ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. As further clarified in the Directive, the "measures" adopted to remove or block websites containing child pornography, for example where the server is hosted outside of EU territory, can be based on both legislative and non-legislative actions. In this regard the Directive is encouraging the internet industry to prevent the misuse of its services with various tools, e.g. self-regulation. Whichever basis of action is chosen, Member States should ensure legal certainty for both service providers and users.[94] According to a report published by the Commission on the implementation of this Directive[95], Member States have developed procedures based both on national criminal law and on the ECD.

The notice and action procedures for illegal content based on the ECD can be activated by individual users who can contact national authorities through the use of e.g. hotlines. National authorities subsequently locate the website, assess its content, and notify the service provider of the existence of illegal content on its website. The Directive does not set a clear timeframe for the removal of content flagged by the authorities, nor does it prescribe penalties for non-compliance with the removal notification. Both timeframe and penalties are explicitly defined in the proposed Regulation on terrorist content.

## 2.6 Soft law measures to tackle illegal content

Besides these legislative measures, additional soft law measures in order to tackle illegal content online have been launched, mainly initiated by the EU Commission. Among the most relevant are the Code of Conduct on countering illegal hate speech online (see Section 2.6.1) and the Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online (see Section 2.6.2. below).

---

90 Directive 2011/93/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.
91 Art. 14 ECD.
92 Art. 25 (1) of the Child Abuse Directive.
93 Art. 25 (2) of the Child Abuse Directive.
94 Recital 47 of the Child Abuse Directive.
95 COM(2016) 872 "assessing the implementation of the measures referred to in Art. 25".

### 2.6.1 The Code of Conduct on countering illegal hate speech online

This Code of Conduct[96] was drawn up in 2016 on the initiative of the Commission. It is a legally non-binding list of public commitments by several IT companies (e.g. Facebook, Twitter, Youtube, Instagram, Google+) to prevent illegal hate speech[97] on the Internet. The Code was agreed with the Commission and serves not only as a guideline for the IT companies' own activities, but also as an exchange of best practices with other IT companies, platforms and social media operators. It includes, among other things, a voluntary commitment to introduce procedures and resources for reviewing notifications of illegal hate speech and to review the majority of valid notifications within 24 hours and, where appropriate, to remove or disable access to such content. The IT companies also undertake to establish national contact points, to communicate speedily and effectively with competent national authorities, to raise awareness and educate users which content is not permitted under their rules and to cooperate with third parties e.g. civil society organisations. Third parties monitor commitment to the code of conduct on a regular basis and report to the Commission.[98] According to the fourth evaluation on the Code of Conduct presented by the Commission in February 2019[99], 72% of the notifications deemed to be illegal hate speech were removed. 89% of the notifications where assessed in less than 24 hours.

### 2.6.2 The Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online

On 1 March 2018, the Commission has adopted Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online. The recommendation does not affect the ECD and other existing legislative measures and the rights and obligations resulting therefrom. It encourages Member States and mainly hosting service providers to take effective, appropriate and proportional measures to tackle illegal content online, while acting in full compliance with EU law and in particular with the fundamental rights laid down in the CFR, including the right to freedom of expression and information. The Recommendation follows up on the Commission's "Illegal Content Communication" [Communication COM (2017) 555 on tackling illegal content online[100]] and builds on the different voluntary initiatives to free the internet from illegal content.[101]

The Recommendation sets out certain main principles that should guide the activities of the Member States and of the concerned service providers in the interest of an effective fight against illegal content online and in order to safeguard the balanced approach of the ECD.[102] It defines "illegal" content as "any information which is not in compliance with Union law or the law of a Member State concerned".[103] When implementing the recommendations, the following factors should be taken into account: the seriousness of the illegal content as well as the type of potential harm caused by it – which

---

96 Available under https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.

97 Illegal hate speech means all conduct publicly inciting violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin, see Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

98 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#monitoringrounds.

99 https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf.

100 Communication COM(2017) 555 of September 2017 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.

101 See Chapter I 1 – 3. of Recommendation (EU) 2018/334.

102 Recital 12 of Recommendation (EU) 2018/334.

103 Chapter I.4. of Recommendation (EU) 2018/334.

depends on how swift possible actions can be taken – and what can reasonably be expected from hosting service providers, considering the potential use of available technologies.[104]

Chapter II of the Regulation contains general recommendations which relate to all types of illegal content. Inter alia, the Commission recommends the following:

- There should be user-friendly procedures for the transmission of notices, encouraging the submission of notices which are sufficiently precise and substantiated to enable the respective hosting provider to take an informed and diligent decision on whether the content is illegal or not.
- There should be fast-track procedures to process notices submitted by competent authorities.
- Hosting service providers who decide to remove or disable access to any content should inform the affected content provider promptly of that decision, the reasons for taking it and of the possibility to contest the decision, except where the illegality of the content is manifest or a competent authority asks the provider not to do so e.g. for reasons of public security.
- Content providers should have the possibility to easily contest the decision through the submission of a counter-notice to the hosting service provider. The latter should then consider whether the content in question is not to be considered illegal, and possibly reverse its decision to remove or disable access to it.
- Hosting services providers should be encouraged to publish a detailed explanation of their policy with regard to the removal of illegal content as well as yearly reports on their activities to remove and disable content.
- Hosting service providers should be encouraged to take appropriate, proportionate and specific proactive measures in respect of illegal content, which could involve the use of automated means for the detection of illegal content, subject to effective and appropriate safeguards. The Commission confirmed its view105 that voluntary proactive measures taken by online platforms falling under Article 14 of the ECD to detect and remove illegal content – including the use of automatic tools and tools meant to ensure that previously removed content is not re-uploaded – do not lead to a loss of the liability exemption. In particular, the Commission stated that the taking of such measures need not imply that the online platform concerned plays an active role which would no longer allow it to benefit from that exemption.
- In order to avoid the erroneous removal of legal content, effective and appropriate safeguards should ensure that hosting service providers act in a diligent and proportionate manner when deciding on the possible removal or disabling of access to content.
- Where hosting providers use automated means, effective and appropriate safeguards such as human oversight and verifications should be provided to ensure that decisions to remove or disable access to content are accurate and well-founded, in any case where a detailed assessment of the relevant context is required in order to decide whether or not the content is to be considered illegal content.
- Cooperation between hosting providers and so-called “trusted flaggers” which should be determined based on their expertise according to clear and objective conditions should be encouraged and there should be fast-track procedures to process notices submitted by them.

[104] Recital (14) of Recommendation (EU) 2018/334.
[105] This view was already set out in its Communication COM (2017) 555 on tackling illegal content online (Fn. 100).

- Hosting service providers should share experiences, technological solutions and best practices to tackle illegal content online among each other and in particular with smaller providers.

Chapter III of the Recommendation contains specific recommendations relating to terrorist content. The proposed Regulation on preventing the dissemination of terrorist content[106] builds upon these recommendations; nevertheless, the latter will remain in force.[107]

## 2.7 Evolving new legislation in the EU Member States

In addition to the sector-specific legislation at EU-level, Member States are responding to the growing prevalence of hate crime and other criminal content on the internet, particularly on social networks such as Facebook, YouTube and Twitter. Some Member States have moved forward and have passed or are discussing their own national laws, inter alia introducing compliance rules for social network providers on how to deal with user complaints about hate crime and other criminal content on the internet.

### 2.7.1 German Netzwerkdurchsetzungsgesetz

A major example is the German Netzwerkdurchsetzungsgesetz (Law on improving law enforcement in social networks, hereinafter: "NetzDG") in force since October 2017. This law aims to combat unlawful content such as hate crime, punishable false messages and other punishable content – e.g. insults – on social network platforms more effectively.[108] To reach this aim, the NetzDG obliges providers of social networks such as Facebook or Twitter inter alia to

- maintain an effective and transparent procedure for handling user complaints about unlawful content,
- remove or block access to "manifestly unlawful" content within 24 hours after receipt of a complaint, and
- to remove or block access to other unlawful content that is not obviously illegal within seven days of receiving the complaint; this time limit may be exceeded in more complex cases.

If the operators systematically fail to meet their obligations, they will face fines amounting to millions of euros.

### 2.7.2 French Loi Avia

Another example is the French "Proposition de loi contre les contenus haineux sur Internet" (Proposal for a law aimed at combating hate content on the internet, also known as "Loi Avia"), approved by the National Assembly and Senat, waiting for the agreement of both chambers on a common text[109]. The legislator wants to curb hate speech and violence on the internet, further involving the economic operators concerned and setting up the Higher Audiovisual Council as a regulatory authority in the

[106] See Section 2.5.4.
[107] See Sect. 2.1 of the proposal COM(2018) 640 for a Regulation on preventing the dissemination of terrorist content.
[108] See https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html.
[109] https://www.franceinter.fr/suppression-des-contenus-filtrage-ce-qui-va-vraiment-changer-avec-la-loi-contre-la-haine-en-ligne.

matter. The proposal is based upon the German NetzDG. To reach its goal, it will impose inter alia these obligations on the operators of the online platforms concerned:[110]

- obligation to remove certain content that is manifestly illegal within 24 hours following a notification;
- obligation to implement a mechanism whereby either the author of the content or the notifier may challenge the decision adopted by the platform;
- obligation to appoint a legal representative located on French territory;
- the financial penalty incurred for failure to meet these obligations must be pronounced by the Higher Audiovisual Council and amount to a maximum of 4 % of the service provider's global annual turnover;
- internet service providers, search engines and domain name providers are also obliged, on the order of the competent administrative authority, to block access to any site providing certain content that has already been deemed illegal by court ruling.

## 2.8 Weaknesses of the existing framework

As revealed in this Section, the current regulatory framework for online services with the ECD as its centrepiece that also introduces specific exceptions from liability has evolved over the past twenty years, through sectoral legislation and a growing body of jurisprudence from the CJEU.

While some regulatory loopholes were already evident when the ECD was adopted[111], the development of the internet over the past two decades has led to the emergence of new services which raise questions on the applicability and interpretation of the ECD and its liability rules. In recent years, besides some soft law measures, sectoral legislation has been introduced, creating fragmented and varied regimes for the take-down of illegal content applicable to hosting providers (e.g. the new liability exemption regime of the Copyright Directive 2019 which differs from the ECD's liability exemption regime). Furthermore, national legislation covering the removal of unlawful content is in place (e.g. in Germany) or under discussion (e.g. in France).

In summary, the foregoing analysis indicates significant **legal uncertainty** about the application of the ECD and its intermediary liability regime on quite a number of providers. In particular, the following uncertainties remain:

(1) It is unclear whether search engine operators, providers of hyperlinks and new service providers such as cloud service providers and providers of collaborative platforms can benefit at all from the ECD's liability exemptions. Without clear harmonised rules at EU level, these services are subject to different national laws and thus different liability rules in the Member States.

(2) Even if these providers are covered by the scope of the liability exemptions, it is unclear when they meet the conditions for these exemptions:
   - For example, it is unclear how the term "actual knowledge" should be interpreted. Is knowledge of the existence of the information on the platform already sufficient, or must the provider also have knowledge of its illegality?

[110] https://ec.europa.eu/growth/tools-databases/tris/en/index.cfm/search/?trisaction=search.detail&year=2019&num=412&mLang=EN.
[111] See Section 2.2.4.

- According to the current concept of active or passive provider, only "neutral" or "passive" providers benefit from the liability exemption. It is not always clear, however, when a provider plays an "active" or "passive/neutral" role. As the threshold separating passive from active behaviour is unclear, this concept of the active or passive provider is often difficult to apply, especially to new services and platforms offering a large number of interrelated services. In its comprehensive case law, the CJEU has introduced more nuances of meaning to this concept and set some guidelines in individual cases. However, not only it is challenging for the providers to fully comprehend this case law, national courts who decide on the provider's role may also come to diverging interpretations and conclusions.

(3) The ECD obliges intermediaries to remove information or block access to it upon obtaining knowledge of its illegality, without establishing detailed and uniform rules on the applicable notice and action procedure. The sector-specific legislation – in place or in the process of approval – has created different regimes for the notice and action procedure for specific types of illegal content, e.g. copyright infringing material or terrorist propaganda. It does not, however, contain fully comprehensive rules; e.g. the proposed Regulation on terrorist content only foresees duties to remove content flagged by authorities, not by users. It is also unclear when providers act "expeditiously" to remove or block illegal content. National courts and legislators – as in the case of the German NetzDG and the French Draft Loi Avia[112] – are filling regulatory loopholes and – inter alia – starting to establish diverging rules and timeframes for the removal of illegal content. There are increasing differences between emerging national rules on notice and action mechanisms.[113]

(4) The ECD grants the provider an exemption from liability as long as the provider is unaware of illegal content being hosted. The ECD does not prohibit proactive monitoring on the service provider's own initiative. Providers are thus free to voluntarily take such proactive measures ("good Samaritan actions") in order to discover and remove illegal content hosted on their platforms, even before it is reported to them by the responsible authority or an internet user. The problem is, however, that such proactive monitoring may result in the provider obtaining knowledge of the illegal content or activity, or at least becoming aware of facts or circumstances from which the illegality is apparent. This could result in loss of the liability exemption for hosting providers where the provider fails to expeditiously block or remove the respective content.

(5) There are open questions regarding the permissible scope of injunctions and the possible degree of obligations that may be imposed on providers by national courts. The ECD allows Member States to impose monitoring obligations on providers in specific cases, and national courts may order providers to terminate or prevent infringements. On the other hand, the ECD prohibits Member States from imposing on intermediaries a general obligation to monitor the content they host. National courts have however in recent years imposed more and more injunctions on intermediaries obliging them to prevent particular infringements, which implies a certain degree of monitoring. There remains uncertainty over the differences between (allowed) "specific" and (forbidden) "general" monitoring obligations, or, in other words, what

[112] See Section 2.7.
[113] See Recital 11 of Recommendation (EU) 2018/334.

degree of monitoring a "specific" obligation may entail, and when such a "specific" obligation imposed in an injunction in effect amounts to a general monitoring obligation.

These ambiguities may have the following possible consequences:

While unclear rules for digital services create legal uncertainty, different national interpretations of existing rules or the creation of new different legal rules for identical services lead to a legal fragmentation within the internal market. As a consequence, not only are internet users and rightsholders protected differently in different countries against illegal content, but also the EU-wide fight against illegal content is rendered ineffective, resulting in a lack of effective protection of internet users and rightsholders. Legal uncertainty and fragmentation are also likely to increase the costs for service providers. This is especially burdensome for small innovative companies who might face challenges in scaling up and expanding in other Member States, making it difficult for them to compete e.g. with big existing market players or U.S. startups.

Besides these ambiguities, the following general issues of the current regime have to be taken into account:

(1) The ECD applies only to service providers established within a Member State, not to service providers from third countries. There is no EU-wide coordinated approach to third country service providers; each Member State may define its policy with respect to those providers, provided that this policy conforms with international trade agreements.[114] This renders the tackling of illegal content stored by such providers in the EU more difficult.

(2) Regulatory competence and oversight for digital services in the EU is currently split between different sectoral regulators (e.g. data protection authorities, regulators of audiovisual media services, competition authorities, regulators of electronic communication services and consumer protection authorities). Furthermore, the technical process is racing ahead, and new services are evolving extremely fast and giving rise to more and more complex questions. It is therefore difficult to ensure a quick, consistent and effective oversight and enforcement of the rules on digital services.

(3) While the ECD's general principles of a prohibition of general monitoring obligations and liability exemptions for intermediaries are respected both by the jurisprudence and the sector-specific legislation at EU level, the evaluation of the case law on the ECD and the new legislation on national and EU level shows that there is a certain tendency to impose more or stricter specific obligations on service providers to act in order to tackle illegal content. Inter alia,

- providers must act to prevent their own infringements, e.g. by negotiating licenses (Copyright Directive);
- providers must take measures to identify suspicious content (Regulation on marketing and use of explosive precursors);
- providers must remove notified content promptly or within very limited time limits (child pornography/terrorist content);

[114] See communication COM(2001) 66 final, p. 6.

- commercial wifi operators can be ordered in an injunction to use technical means such as password protection to prevent the users of their wifi from committing copyright infringements (CJEU – Mc Fadden);
- hosting providers can be ordered to remove, not only specific unlawful information, but also future information with identical content or even information with only equivalent – but essentially unchanged – content which contains certain elements specified by the court (CJEU – Glawischnig Piesczek).

This may have the following possible consequences:

- These duties might pose a huge financial or organisational burden on smaller providers.
- The removal of illegal content falls more and more within the area of responsibility of private parties, in particular huge service providers, who gain more control over the content available via their platforms. Unlike public authorities and regulators, however, private actors are not directly bound by fundamental rights. It is therefore questionable whether an adequate protection of fundamental rights, in particular the freedom of expression and information, can be ensured. Member States including their legislative, executive and judicial powers have inter alia the negative obligation not to interfere with fundamental rights. Therefore, they have to make sure that any limitations of fundamental rights are prescribed by law, pursue a legitimate aim and are necessary in a democratic society. This does not, however, apply to private platform operators, even though they inter alia have the power to decide about making available, keeping or removing content on their platforms. This may harbour risks, in particular for the fundamental right freedom of expression and information, unless adequate safeguards for fundamental rights and effective remedies are also envisaged.
- It is getting harder for providers to fulfil the conditions of the ECD's liability exemptions and to remain non-liable for third party content, or at least this cannot be excluded.
- Increased liability risks may trigger over-blocking of critical but lawful content, as providers might simply take such content down instead of exposing themselves to liability, without properly checking the legality of such content or taking other appropriate measures to protect lawful content.

# 3 Possible plans of the EU Commission to address existing problems in a "Digital Services Act"

Given the current legal situation and the weaknesses resulting from it, it is reasonable that the Commission is considering the introduction of new legislation, updating the ECD, with the overarching goal of increasing legal certainty for businesses and consumers alike, and preventing the fragmentation of the internal market. This section will outline how – according to the first ideas internally discussed within the European Commission – the Commission could possibly address the identified problems and shape the future EU legal framework for digital services with regard to service providers' liability for illegal content online.

## 3.1 Political background

As already mentioned in the Introduction, the President of the Commission, Ursula von der Leyen, has been about the first to express the need to introduce a new Digital Services Act (hereinafter "the DSA"). In her Agenda for Europe, she announced that this act "will upgrade our liability and safety rules for digital platforms, services and products, and complete our Digital Single Market".[115] According to the European Commission's Work programme for 2020[116], "*a new Digital Services Act will reinforce the single market for digital services and help provide smaller businesses with the legal clarity and level playing field they need*". The Commission further announces that protecting citizens and their rights, not least the freedom of expression, will be at the core of their efforts.

Margrethe Vestager, Executive Vice-President for a Europe fit for the Digital Age, is supposed to "coordinate the work on upgrading our liability and safety rules for digital platforms, services and products as part of a new DSA"[117]. The Commissioner Thierry Breton is expected to "lead the work on a coordinated European approach on the new DSA".[118]

The Commission announced in its Work Programme for 2020[119] that a draft of the DSA will be released in Q4 of 2020.

## 3.2 Possible content of the Digital Services Act on liability for illegal content online

While no text has been officially rolled out yet, an internal note written by officials in the Commission's Directorate General for Communications Networks, Content and Technology (DG CONNECT) was leaked in July 2019.[120] This document was intended to provide a basis for a discussion at the Digital Single Market Steering Group on "a potential new initiative […] to update the horizontal regulatory framework for all digital services in the single market, in particular for online platforms."[121] It roughly describes the reasons why and the fields where the Commission considers updating or amending the existing legislation.

According to the internal Commission note, the DSA's overall aim is to update, clarify and harmonise the rules for digital services in the EU. This will comprise inter alia

- a "refit" of the ECD into a DSA with clear, uniform, up-to-date and innovation-friendly rules,
- the possible development of the ECD into a regulation.

The paper suggests that the DSA should be built on the existing key principles of the ECD: it will in particular

- strengthen the home state control principle,

---

[115] Ursula von der Leyen, A Union that strives for more – My Agenda for Europe, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf, p. 13. See also cepAdhoc "Von der Leyen's tasks for the new EU Commission – Part 3", November 26, 2019, p. 3.

[116] COM(2020) 37 final, p. 4.

[117] Mission letter to Margrethe Vestager, p. 4.

[118] Mission letter to Thierry Breton, p. 5.

[119] See Annex 1 of the Work Programme, available under https://ec.europa.eu/info/sites/info/files/cwp-2020-annex-1_en.pdf.

[120] The paper was published i.a. on the website of netzpolitik.org, see https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf.

[121] Internal Commission document (Footnote 2), p. 1.

- maintain “the general principle of a harmonised and graduated and conditional [liability] exemption” for intermediaries as a foundational principle of the internet,
- maintain the prohibition of general monitoring obligations as a foundational cornerstone of internet regulation.

Further details are listed in the following table, which connects existing specific problems with the Commission’s initial plans and aims to provide an early insight into what might possibly be the subject of the proposed DSA with regard to liability for illegal content online. However, it has to be noted that this table is based on the content of the leaked internal Commission note from July 2019 and thus may not reflect the current status quo of the discussion within the European Commission.

**Tab. 2: Current specific problems with regard to service providers' liability for illegal content online and possible solutions in the future DSA**

| PROBLEM | DETAILS | Possible consequences | Possible content of DSA to address problem |
|---|---|---|---|
| **Scope** | | | |
| **Unclear if "new" services such as**<br>- **cloud services**<br>- **content delivery networks**<br>- **social media services**<br>- **collaborative economy platforms**<br>- **domain name services**<br>- **online advertising services**<br>- **digital services built on electronic contracts and distributed ledgers**<br>**qualify as information society services and as such fall under the ECD** | • The CJEU has been consulted and taken decisions in individual cases, e.g. on Uber and AirBNB. However, these decisions often contain complex evaluations of the respective platform's interrelated activities and services and their role and thus do not create a clear legal situation for collaborative economy services | • Legal uncertainty<br>• Legal fragmentation<br>• If these services do not fall under the ECD at all, their providers cannot benefit from the liability exemptions. | • **Clarify and update the scope of the ECD**<br>• **Include in the ECD all digital services from internet service providers to cloud hosting services, content delivery networks, domain name services, social media services, search engines, collaborative economy services, online advertising services and digital services built on electronic contracts and distributed ledgers** |
| **The ECD's rules and obligations apply to all information society services regardless of their market status or power.** | • Although some online platforms have developed excessive market power, they are subject to the same rules as small providers | • Small companies might have difficulties in scaling up | • **Examine options to define a category of services on the basis of a large or significant market status, complementing the competition threshold of dominance, in order to impose supplementary conditions** |
| **The ECD does not apply to services supplied by service providers established only in a third country.** | • The ECD's home state control principle does not apply<br>• There is no EU-wide coordinated approach with regard to third country service providers; each Member State may define its policy with respect to those providers, provided that this policy conforms with international trade agreements | • Legal fragmentation<br>• This renders the tackling of illegal content stored by such providers more difficult and less effective. | • **Assess the need to expand the scope of the DSA to service providers established in third countries**<br>• **Simplify establishment of service providers in the EU, e.g. by mandating a single digital representative instead of possibly a representative for each Member State in which the service providers operate** |

| **Liability** | | | |
|---|---|---|---|
| **Unclear if the providers of the following services fall under the ECD's liability exemptions for intermediaries:**<br>- **search engine operators,**<br>- **providers of hyperlinks,**<br>- **providers of "new" services" such as**<br>  - **cloud services**<br>  - **content delivery networks**<br>  - **social media services**<br>  - **collaborative economy platforms**<br>  - **domain name services**<br>  - **online advertising services**<br>  - **digital services built on electronic contracts and distributed ledgers** | • The ECD leaves the liability of search engine operators and providers of hyperlinks expressly open, leaving Member States to regulate the issue<br>• The CJEU has ruled that providers of paid internet referencing systems (Google Adwords) can be exempted from liability like hosting providers if they play a neutral and not active role, but national courts decide on the qualification of their role<br>• The liability of providers of classic search engines is still unclear<br>• Unclear whether and under what conditions "new" services fulfil the criteria for access, caching or hosting providers, or should be treated in the same way in order to profit from liability exemptions | • Legal uncertainty<br>• Legal fragmentation due to differing national laws and court rulings | • **Update the liability provisions of the ECD, taking stock of the nature of services in use today and of the sector-specific legislation adopted at EU level**<br>• **Possibly expand liability exemptions for access, caching and hosting providers explicitly to search engine operators and providers of hyperlinks**<br>• **Codify existing case-law**<br>• **Clarify application of and possibly expand liability exemptions for access, caching and hosting providers to some providers of "new" services, e.g.**<br>  - **cloud services**<br>  - **content delivery networks**<br>  - **collaborative economy services**<br>  - **domain name services;** |
| **Liability is currently based on the concept of the "active" or "passive" provider** | • Current law makes liability exemption for hosting providers dependent on the nature of the activities of the provider (concept of active or passive/neutral hosting provider)<br>• Only neutral/passive providers profit from the liability exemptions (they are deemed to have a lack of knowledge or control of the stored information)<br>• If a provider exceeds the threshold of a certain "activity", he is deemed to be an "active" provider and falls out of the scope of the liability exemption unless it acts expeditiously to block access or take down the content in order to remain exempt from liability | • Concept of active and passive providers is not fully clear<br>• Application of this concept to new services such as collaborative economy services (AirBNB, Uber) is questionable and complicated as these service providers offer more and more related, overlapping and ancillary services which augments their risk to be qualified rather as an "active" provider (and | • **Replace concept of active/passive hosting providers by more appropriate concepts building rather on notions such as whether the providers have**<br>  - **editorial functions**<br>  - **actual knowledge and**<br>  - **a certain degree of control** |

| | | | |
|---|---|---|---|
| | • The CJEU has set some guidelines in individual cases – e.g. on Uber, AirBNB and Google Ads –, but national courts decide on the qualification of the provider's role as active or passive | not as a "passive" provider who can benefit from the liability exemptions)<br>• Complex jurisprudence of CJEU in individual cases, but no clear and simple harmonised rules<br>• Legal uncertainty<br>• Legal fragmentation | |
| **There are no EU-wide detailed rules on the applicable "notice and action" procedure for the removal of illegal content** | • The ECD obliges intermediaries to remove or block content upon obtaining knowledge of its illegality but does not contain detailed rules on the applicable notice and action procedure<br>• Sectoral legislation does not contain uniform comprehensive rules either (e.g. Regulation on terrorist content only contains obligations to remove content flagged by competent authorities, not by users) | • Legal fragmentation: Member States and national courts fill the gaps and establish diverging rules and timeframes for the removal of illegal content (German NetzDG, French draft Loi Avia)<br>• Risk that illegal content is not effectively tackled, with the risk of reputational or other damage<br>• Freedom of expression and information may be at risk if practices to remove illegal content differ and there are no EU-wide rules on appropriate measures to protect lawful content | • **Create uniform, EU-wide binding rules on the applicable notice and action procedure for the removal of illegal content (e.g. illegal hate speech)**<br>• **Consider tailoring such rules to the types of services (e.g. mere access providers, social networks, collaborative economy services)**<br>• **Possibly continue tailoring such rules to the types of content in question, where necessary (e.g. hate speech, copyright infringing content)**<br>• **Consider making the applicability of the rules subject to thresholds where feasible; depending on**<br>- **the service provider's size and nature and**<br>- **the nature of its potential obligations**<br>• **Maintain the maximum simplicity of rules**<br>• **Include "a robust set of fundamental rights safeguards"** |

| | | | |
|---|---|---|---|
| **Providers also become liable when they gain knowledge/awareness as the result of own investigations** | • Providers have no incentive to act proactively to tackle illegal content and adequately address harmful content ("good Samaritan actions"), as they might risk becoming liable<br>• If providers decide to take action beyond legal obligations and face the risk of liability, they have limited legal incentive for taking appropriate measures to protect lawful content (risk of overblocking) | • Illegal content is not sufficiently and effectively tackled and remains longer online, with the risk of reputational or other damage<br>• Freedom of expression and information is at risk | • **Include a binding "Good Samaritan provision"**<br>• **Encourage and incentivise proactive measures to attack illegal content**<br>• **Clarify the lack of liability as a result of such measures**<br>• **Build on the notions already included in the Illegal Content Communication COM(2017) 555** |
| **The general principle regarding the prohibition of general monitoring obligations is still in place, but providers' duties and liability risks are nevertheless constantly increasing** | • Liability for own infringing action (trademark law, copyright law) has been expanded – since this is no longer a question of secondary liability, no liability exemption applies in this regard<br>• Liability for omissions (failure to act when notified) has been increased<br>• More complex "specific" monitoring duties have been introduced (via injunctions), e.g. the obligation not only to remove identical, but also "equivalent" information | • Risk for freedom of services / internet<br>• Upload filters may be used, but there are no EU wide rules to protect lawful content (risk for freedom of expression) | • **Provide transparency and accountability with regard to the use of automated filtering technologies**<br>• **Consider specific provisions governing algorithms for automated filtering technologies, where these are used.**<br>• **Maintain the prohibition of general monitoring obligations** |
| **Oversight and Enforcement of Rules** | | | |
| **No effective public oversight and enforcement**<br><br>**Lack of timely regulatory control** | • Regulatory competence and oversight are currently split between different sectoral regulators (e.g. data protection authorities, regulators of audiovisual media services, competition authorities, regulators of electronic communication services, consumer protection bodies), and is sometimes contradictory | • Online platforms have become de-facto regulators without adequate and necessary oversight | • **Adopt measures to ensure adequate and appropriate oversight of providers of digital services in the EU and enforcement of the rules, in particular for cross-border situations**<br>• **This includes the creation of a new regulatory structure. Depending on the specific mission, this could be**<br>**- a central regulator,**<br>**- a decentralised system, or**<br>**- an extension of powers of existing regulatory authorities.** |

| | | | |
|---|---|---|---|
| | • There is no specific regulator for platforms in the EU<br>• Rules – e.g. specific monitoring obligations –are not always easy to fulfil | | • **This also includes the exploration of possible roles and powers of such regulatory structures, including**<br>- **reporting requirements,**<br>- **powers to require additional information,**<br>- **complaint handling,**<br>- **the power to impose fines or other corrective action, or**<br>- **approvals of codes of conduct**<br>• **Provide regulators with appropriate digital capacities and competences**<br>• **Give providers guidance for emerging issues, e.g. help translate rules into technical solutions** |

# 4 Summary

The EU Commission announced it will propose in the fourth quarter 2020 a Digital Services Act ("DSA"). The DSA will tackle specific problems of the current legal framework by updating liability and safety rules for digital services, platforms, and products. In summer 2019, an internal Commission note was leaked, outlining possible measures how the Commission might address these problems. This cepStudy analyses the weaknesses of the current legal framework regarding service providers' liability for illegal content online. These weaknesses are then linked to the possible measures of the DSA that are outlined in the leaked Commission note.

The centrepiece of the current regulatory framework for digital services is the E-Commerce Directive (ECD). This directive introduces specific exemptions from liability, which also affect providers' liability for illegal content online, as well as duties for certain digital services, so called "information society services". In parallel with the technical progress, new types of digital services have emerged that were not envisaged when the ECD was adopted. Inter alia, social media and other online platforms are today being widely used to generate and exchange content and thus also facilitate the dissemination of illegal content. Intermediaries such as hosting providers that store such content play a central role acting as gatekeepers, which raises questions on their responsibilities with regard to the dissemination of illegal content via their platforms. Over the past twenty years, the ECD was therefore complemented by sectoral legislation, soft law measures and a growing body of jurisprudence from the Court of Justice of the European Union (CJEU). Currently, the strategy to tackle illegal content in the EU is characterized by fragmented approaches and remaining legal uncertainty, which incites more and more Member States to adopt national legislation, creating a risk of further legal fragmentation. In particular, the following uncertainties remain:

Currently, it is unclear whether "new services" such as cloud services, social media services or collaborative economy platforms qualify as "information society services" and therefore fall under the ECD. This leads to legal uncertainty for providers of such services. The DSA might therefore clarify and update the scope of the ECD, so to include new services.

At present, the ECD's duties apply to all information society services regardless of their market power. For providers with large market power it is often easier to fulfil these duties than for new providers. New providers might therefore have problems to scale up. The DSA might therefore examine options to define different duties for providers depending on the market power.

The ECD does not apply to services supplied by providers established only in a third country. Therefore, each Member State defines its policy with respect to those providers. This leads to legal fragmentation and renders the tackling of illegal content stored by such providers more difficult and less effective. The DSA might therefore expand the scope of the ECD to service providers established in third countries that offer their services within the EU.

For some providers of digital services – e.g. search engine operators, providers of hyperlinks or providers of "new services" such as cloud services and content delivery networks – it is unclear whether they may benefit from the ECD's liability exemptions. This leads to legal uncertainty regarding their liability for illegal content online. The DSA might therefore update the liability provisions of the ECD and possibly expand its liability exemptions expressly to search engines and wifi hotspots, and clarify their application to "new" digital services.

In the current regulatory framework, liability exemptions depend on the nature of the activities of the provider. Only "passive providers" profit from the liability exemptions as they are deemed to have a lack of knowledge or control of the stored information. If a provider exceeds the threshold of a certain "activity", it is deemed to be an "active" provider and falls out of the scope of the liability exemption unless it acts expeditiously to block access to or remove the content. There are no harmonised rules in the EU that define when a provider is deemed to be active and passive. Although the CJEU has set some guidelines in individual cases – e.g. on Uber, AirBNB and Google Ads –, national courts decide on the qualification of the provider's role as active or passive. As the jurisprudence of CJEU is very complex and case specific, national courts can interpret it differently. This leads to legal fragmentation throughout the EU. Beyond this, providers offer more and more related ancillary services which could make them appear rather "active". The DSA might therefore replace the concept of active/passive providers by a more appropriate concept.

In addition, providers currently have little incentive to act proactively to tackle illegal content: they might face the risk of becoming liable when gaining knowledge or awareness of such illegal content as the result of their investigations, unless they act expeditiously to remove or block access to that content. If providers do not act proactively, illegal content is not sufficiently and effectively tackled and remains longer online. In contrast, if providers do decide to act proactively, the liability risk leaves them little incentive to take appropriate measures to protect lawful content, which causes a risk of overblocking. The DSA might clarify the lack of liability as a result of proactive measures and include a binding "good Samaritan provision" in order to encourage such measures.

The ECD obliges providers to remove or block content upon obtaining knowledge of its illegality but does not contain detailed rules on the applicable notice and action procedure. Sectoral legislation to remove illegal content e.g. terrorist content or content that infringes copyrights does not contain uniform comprehensive rules either. In order to prevent legal fragmentation by emerging national legislation, the DSA might create uniform, EU-wide binding rules on the applicable notice and action procedure for the removal of illegal content, including robust safeguards for the protection of fundamental rights. Nonetheless the Commission might continue tailoring such rules to the types of content in question, if necessary.

The ECD prohibits to impose "general monitoring" obligations for illegal content online to providers. However, the ECD does not prohibit monitoring obligations on providers in "specific cases" duties. Over the past twenty years, more and more duties to prevent particular infringements have been imposed on providers (via sectoral legislation or injunctions), which imply a certain degree of "specific" monitoring. Examples are the obligation to remove a specific copyright-infringing content or the obligation to remove not only identical content, but also content which is "equivalent" to the one that was ruled to be illegal. The DSA might consider certain provisions governing algorithms for automated filtering technologies – "where these are used", while maintaining however the prohibition of general monitoring obligations.

Currently, regulatory competence and public oversight are split between different sectoral regulators, e.g. data protection authorities, competition authorities, regulators of electronic communication services and consumer protection bodies. There is no specific regulator for platforms in the EU. Beyond this, new services are evolving very fast and give rise to more and more complex questions. As a result, public oversight and enforcement of the current legislation is ineffective. Online platforms have become de-facto regulators with more and more powers, but without adequate and necessary oversight.

The DSA might therefore adopt measures to ensure adequate and appropriate oversight of providers of digital services in the EU and enforcement of the rules, in particular for cross-border situations. This might include the creation of a new regulatory structure.

**cep | Centre for European Policy**
Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Germany
Phone +49 761 38693-0 | www.cep.eu