Online platforms and services

QUECK, Robert; Kuczerawy, Aleksandra; Ledger, Michele

Published in:
Electronic communications, audiovisual services and the Internet

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

ONLINE PLATFORMS AND SERVICES

Alexandre de Streel, Aleksandra Kuczerawy and Michèle Ledger

Introduction Online platforms span a wide range of activities, from online market places, to search engines, social media, platforms for the collaborative economy and app stores. According to the Commission, the main characteristics of these players are that they have the ability to create and shape new markets, they operate in multisided markets, they benefit from network effects and they play a key role in the digital value creation.[1] Online platforms do not fall under the framework of specific sector specific legislation. Many of the online platforms provide "information society services" which implies that they are covered by the relatively light touch rules of the Electronic Commerce Directive, while also benefiting from the country of origin and liability exemption.[2] However, when the online platforms provide specific types of information society services (such as communications services, video and content sharing, intermediation or search engines), they are subject to additional obligations. Moreover, just like any other service provider, they also need to comply with horizontal legislation such as personal data protection, consumer protection or competition law. 3-001

A. DIFFERENT CATEGORIES OF ONLINE SERVICES

Different shades of information society services Online platforms have developed many types of business models but often they provide "information society services" which are defined very broadly under EU law. This broad category may be sub-divided into narrower categories of information society services which are subject to specific obligations, linked to the characteristics and the risks raised by each sub-category. 3-002

1. Online services in general

(a) Information society services

Information society services They are defined by the Regulatory Transparency Directive[3] as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient". The key elements in 3-003

---

1 Communications of the Commission of 25 May 2016 on online platforms and the Digital Single Market Opportunities and Challenges for Europe, COM(2016)288, p.3.

2 Directive 2000/31 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 [2010] OJ L178/1.

3 Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services [2015] OJ L241/1. The Directive sets up a procedure whereby

the definition are (i) the service must be provided for remuneration; (ii) at a distance; (iii) by electronic means; and (iv) at the individual request of the recipient of the service.

3-004 **Normally provided for remuneration** Remuneration is a standard condition for services under EU law.[4] The remuneration does not have to come directly from the recipient of the service and covers non–monetary means of payment such as personal or non-personal data.[5]

3-005 **At a distance** This means that the service must be provided without the parties being simultaneously present.[6] Many types of online services are therefore covered such as search engines, news and weather services, social media platforms, online educational services, online shopping and booking services. However, the consultation of an electronic catalogue in a shop with the customer present in the shop is not a service provided at a distance. Likewise, the reservation of a plane ticket at a travel agency in the physical presence of the customer by means of a network of computers does not satisfy this condition.[7]

3-006 **By electronic means** The service must be sent initially and received at its destination by means of electronic equipment used for the processing (including digital compression) and storage of data, and be entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means. Examples of services covered are online entertainment services offered on the internet, music streaming services, video on demand, betting and gaming, electronic mail, discussion forums, file transfer and online validation services. However, voice telephony services and other services provided via voice telephony are therefore

Member States must notify to the European Commission all draft technical regulations on products and information society services before they are adopted in national law. Since these measures can lead to trade barriers, Member States must ensure that they act in a transparent manner, by giving the Commission and the other Member States the possibility to react. The notification triggers a three-month standstill period to allow the Member States and/or the Commission to react. If there is no reaction, the member state can adopt the measure after the three-month standstill period has expired. If the Commission or a Member State issues a comment, the Member State does not need to reply formally but it must take the comments into account as far as possible. It can adopt the technical regulation after the three-month standstill period has expired. Where the Commission or a Member State sends a detailed opinion (if it considers that the technical regulation creates obstacles to the freedom to provide information society services (or the free movement of goods) the Member state must take into account the detailed opinion and reply to it by explaining what it intends to do. The standstill period is extended to four months in the case of information society services and allows for a dialogue to take place between the Member States and the Commission, with the possibility for the Commission to request the postponement of the adoption of the draft. Article 1.1.b defines the notion of information society service and Annex 1 of the Regulatory Transparency Directive contains an indicative list of services that are not covered by the definition. Guidance is also given by the Commission on the interpretation of the definition of information society services in a Vademecum published on Directive 98/48/EC (the previous regulatory transparency directive which contained the same definition).

4 In particular, art.57 TFEU on the free movement of services and EECC art.2(4) for electronic communications services, analysed in para.2-007 of this book.

5 The case law of the Court of Justice, under art.57 TFEU, considers that there is a remuneration when the service provider is paid by a third party and not by the service recipient: *Deliège* (C–51/96 and C–191/97) EU:C:2000:199, paras 56 and 57 and *Sotiris Papasavvas v Fileleftheros Dimosia Etairia* (C–291/13) EU:C:2014:2209, para.30.

6 Regulatory Transparency Directive art.1.1.(b)(i).

7 Regulatory Transparency Directive Annex 1.

excluded because they are not provided via electronic processing/inventory systems.[8]

At the individual request of the recipient of services The service must be provided through the transmission of data on individual request, meaning that point to multipoint transmissions such as television and radio broadcasting services are not covered by this definition. Video-on-demand services are provided on individual request of the recipient of the service and are therefore also information society services.[9] **3-007**

(b) Collaborative economy platforms

Legal qualification of collaborative economy platforms The qualification of a collaborative economy platform as a provider of information society services and/or as a provider of the underlying service (such as transport for Uber or hosting for Airbnb) has triggered an intense legal and political debate.[10] According to the Commission, the qualification should be established on case-by-case basis and depends on the business model of the platform, in particular the level of control and influence the platform has on the provision of the underlying service.[11] If the level of control or influence is important, the platform should be qualified as the provider of the underlying service. Conversely, if the platform merely assists in providing the underlying service, for instance in matching demand and supply, the platform is merely an information society provider. **3-008**

Court of Justice: Uber This line of reasoning was followed by the Court of Justice when deciding the qualification of UberPOP, the initial unlicensed peer-to-peer taxi service of Uber which connects through an app a person wanting a ride with a non-professional driver using his or her own car. The Court of Justice observed that this is a mixed service, with an element that is provided by electronic means and a "material" element.[12] The Court of Justice also noted that the service goes beyond the provision of an information society service because the platform also offered a transport service which was accessible through the app. In particular, the Court took into account the fact that Uber provided drivers with an app which if it was not used, the transport service would not have taken place, and that Uber exerted a "decisive influence" (Uber set the fare, controlled the quality of the vehicles or set minimum safety standards) over the conditions under which the service was provided. The service in question was therefore qualified as a service in the field of transport, with the consequence that it could not benefit from the favourable regime of the Electronic Commerce Directive or of the Services Directive, which excludes transport services from its scope.[13] **3-009**

Airbnb Following this ruling, a case-by-case analysis therefore needs to be car- **3-010**

8 Regulatory Transparency Directive art.1.1.(b)(ii) and Annex 1.

9 Regulatory Transparency Directive art.1.1.(b)(iii) and Annex 1.

10 Hatzopoulos, *The Collaborative Economy and EU Law* (Oxford/Portland, Hart, 2018).

11 Communication from the Commission of 2 June 2016, A European agenda for the collaborative economy, COM(2016)356, p.6.

12 *Asociación Profesional Élite Taxi v Uber Systems Spain* (C–434/15) EU:C:2017:981; *Uber France* (C–320/16) EU:C:2018:221.

13 Directive 2006/123 of the European Parliament and of the Council of 12 December 2006 on services in the internal market ("Services Directive") [2006] OJ L376/36.

ried out to determine if a given platform provides an information society service or another type of service such as a transport or an accommodation service. In the case of Airbnb, the Advocate General proposed in an opinion in April 2019 that it provides an information society service because the material service (the short-term accommodation market) existed before Airbnb was launched and because hosts can offer rooms through other channels than the service provided by Airbnb. Further, Airbnb does not does not control significant aspects of the accommodation service such as tariffs, the calendar of vacancies and house rules.[14] This means that the more the platform controls the underlying material service (e.g. transport, accommodation etc.), the more likely it will be that the service offered by the platform will not be qualified as an information society service but as the underlying service.

2. Specific categories of online services

3-011 **Communications OTTs** An Over-the-Top ("OTT") communications service or, under EU law terminology, number-independent interpersonal communications service, is a service that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons (whereby the persons initiating or participating in the communication determine its recipient) and which does not connect with publicly assigned numbering resources.[15] Examples are WhatsApp, Skype or Gmail. The online platforms providing this type of services are subject to additional obligations foreseen in the European Electronic Communications Code, in particular regarding interoperability and consumer protection.[16]

3-012 **Video sharing platforms** A video-sharing platform service is a service where the principle purpose (or a dissociable section thereof), or an essential functionality is the provision of programmes and/or of user-generated videos to the general public for which the platform does not have editorial responsibility but determines the organisation of the content (including by automated means or algorithms in particular by displaying, tagging and sequencing).[17] In practice, this targets audiovisual sharing platforms of all sizes and also potentially social media platforms, if the sharing of audiovisual content constitutes an essential functionality of the service and is not merely ancillary to or does not constitute a minor part of the activities of that social media service. According to the revised Audiovisual Media Services Directive, those types of online platforms are subject to additional obligations.[18] In particular, they need to put in place measures to protect minors from harmful content and all citizens from incitement to hatred, violence and terrorism, while also abiding by certain obligations regarding Audiovisual Media Services Directive commercial communications.

3-013 **Online content-sharing service** An online content-sharing service is a service

[14] *Airbnb Ireland* (C–390/18), Opinion of Advocate General Szpunar, EU:C:2019:336.
[15] Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L321/36 ("EECC") art.2(5) and (7).
[16] Those obligations are reviewed in Chapter II of this book.
[17] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services ("Audiovisual Media Services Directive") [2010] OJ L95/1, as amended by Directive 2018/1808 art.1(1aa).
[18] AVMS Directive art.28b, analysed in para.3-085 and paras.4-140 to 4-145 of this book.

whose main, or one of the main purposes, is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, for which the platform organises and promotes the content for profit-making purposes.[19] The online platforms providing this type of service are subject to additional obligations foreseen in the new Copyright in Digital Single Market Directive, in particular regarding liability in case of copyright violation.[20]

3-014 **Cloud computing service** A cloud computing service is an information society service that enables access to a scalable and elastic pool of shareable computing resources.[21] The online platforms providing this type of service are subject to additional obligations foreseen in the Network Information Security Directive, in particular regarding security requirements and incident notification.[22]

3-015 **Online search engines** An online search engine is an information society service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found.[23] The online platforms providing this type of service are subject to additional obligations foreseen in the Regulation on fair treatment of business users of online platforms, in particular regarding transparency[24] and in the Network Information Security Directive, in particular regarding security requirements and incident notification.[25]

3-016 **Online intermediation services** An online intermediation service is an information society service that (i) allows business users to offer goods or services to consumers, with a view to (ii) facilitating the initiating of direct transactions between business users and consumers regardless of whether the transaction is finally concluded offline or online and which (iii) provide services to business users, based on contractual relationships between the platform and the business user.[26] Examples are online e-commerce market places, including collaborative ones (where business users are active), app stores and online social media services. It is not relevant whether the transactions between business users and consumers involve any monetary payment or whether they are partially concluded offline. However, peer-to-peer online intermediation services without the presence of business users or pure business-to-business online intermediation services not offered to consum-

[19] Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9 and 2001/29 [2019] OJ L130/92 ("Copyright DSM Directive") art.2(6).
[20] Those obligations are reviewed in in para.3-086 and Chapter VIII of this book.
[21] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("Network Information Security Directive") [2016] OJ L194/1 art.4(19).
[22] Those obligations are reviewed in paras 6-28 and 6-29 of this book.
[23] Network Information Security Directive art.4(18).
[24] Those obligations are reviewed in para.3-048.
[25] Those obligations are reviewed in paras 6-28 and 6-29 of this book.
[26] Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services ("Regulation on fair treatment of business users of online platforms") [2016] OJ 186/57 art.2(2).

ers are not covered by this definition.[27] The online platforms providing this type of service are subject to additional obligations foreseen in the Regulation on fair treatment of business users of online platforms, in particular regarding transparency and dispute resolution.[28]

3-017 **Online market place** An online marketplace is an information society service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.[29] The online platforms providing this type of service are subject to additional obligations foreseen in the Network Information Security Directive, in particular regarding security requirements and incident notification.[30]

B. AUTHORISATION AND FREE MOVEMENT

3-018 **Introduction** The authorisation regime of online platforms and the extent to which they can benefit from internal market principles depends on the legal qualification of the services they provide. This section covers the framework that specifically applies when platforms provide information society services, and not the underlying other service such as a transport or a hosting service, which may obey radically different rules. The key principle contained in the Electronic Commerce Directive is that the providers of information society services (i) established in the territory of a Member State; (ii) can in principle access the market freely and the Member State where the platform is established; and (iii) must only comply with the national provisions that apply in that Member State; (iv) which fall within the coordinated field of the Electronic Commerce Directive. In turn, the platform cannot face any restriction to the provision of an information society service coming from another Member State but a specific derogation procedure exists which enables Member States to block incoming services which pose a threat to their national legal order.

3-019 **Establishment in a Member State** For these principles to apply, the online platform needs to be established in a Member State by taking into account the case law of the Court of Justice, meaning that it is where the platform actually pursues an economic activity through a fixed establishment for an indefinite period. For websites, this is not the place where the technology supporting the website is located or the place at which the service is accessible, but the place where the service provider pursues its economic activity. If the provider has several places of establishment, for each service, the place of establishment should be determined; in cases where it is difficult to determine from which of several places of establishment a given service is provided, then the place where the provider has their centre of activities for a particular service will prevail.[31]

3-020 **"Free market access"** The market access conditions of information society service providers are contained in the Electronic Commerce Directive. Accordingly, access to the activity of an information society service provider cannot be subject to a prior authorisation, or any requirement having an equivalent effect.[32] Authorisation schemes not specifically targeted at information society services are however allowed.[33]

[27] Regulation on fair treatment of business users of online platforms recital 11.
[28] Those obligations are reviewed in paras 3-040 to 3-047.
[29] Network Information Security Directive art.4(17).
[30] Those obligations are reviewed in paras 6-028 to 6-029 of this book.
[31] Electronic Commerce Directive art.2.c and recital 19.

3-021 **Internal market principle** Each Member State must ensure that information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question. In turn, the other Member States in which the service is provided cannot restrict the incoming service. The Directive introduces a rather complex set of conditions and exceptions to when the principle applies or not. First, it only applies to "the coordinated field" of the Electronic Commerce Directive. On top of that, some areas are altogether excluded from the scope of the Directive, other areas are in scope of the Directive, but are not covered by the internal market clause of the Directive and lastly, it is possible for Member States to derogate from the principle on a case-by-case basis.

3-022 *Coordinated field* A special feature of the Electronic Commerce Directive is that the internal market clause only applies to its coordinated field which is defined in quite some detail in the Directive. It concerns requirements with which the service provider needs to comply for the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification, the pursuit of the activity of an information society service, requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider.[34] In these areas, therefore the platform needs only to comply with the legislation of the Member State of establishment and other Member States could not impose their national rules. The coordinated field however does not cover requirements such as: requirements applicable to goods as such; requirements applicable to the delivery of goods; and requirements applicable to services not provided by electronic means.[35]

3-023 *Areas/activities excluded from the scope of the Electronic Commerce Directive* The main excluded areas and activities are taxation, data protection, competition law, and gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.[36]

3-024 *The internal market principle does not apply to certain areas* These areas are specified in an Annex to the Directive. In practice, the main areas of relevance are matters covered by intellectual property rights, consumer protection and the freedom of the parties to choose the law applicable to their contracts.[37] In these areas, therefore the internal market clause does not apply.

3-025 *Special derogation procedure* This procedure was built into the Directive to al-

[32] Electronic Commerce Directive art.4.
[33] Electronic Commerce Directive art.4(2). Commission First Report of 21 November 2003 on the application of Electronic Commerce Directive, COM(2003)702, p.9.
[34] Electronic Commerce Directive art.2.h i.
[35] Electronic Commerce Directive art.2.h ii.
[36] Electronic Commerce Directive art.1(5).
[37] Electronic Commerce Directive Annex.

low Member States to derogate on a case-by-case basis to the internal market clause and to restrict a specific incoming service from another Member State, where justified. The grounds which justify the triggering of the procedure are wide: any public policy ground in particular, the prevention, investigation, detection and prosecution of a criminal offence, the protection of minors, the fight against any incitement to hatred; the protection of public health; public security and the protection of consumers including investors.[38] The measures taken by the Member State of destination under this procedure need to be necessary in view of one of these reasons, they must be taken against a specific information society service and must be proportionate. A procedure needs to be followed before taking the measure(s) in question, which involves asking the Member State where the service provider is established to take the measure (but has failed to do so) and notifying the Commission and the Member State of establishment of the intention to take the measure. An urgent procedure is also foreseen whereby the Member State of destination is not obliged to contact and notify the Member State of origin or the Commission.[39] However, the procedure has not been used very frequently.[40]

C. OBLIGATIONS OF ONLINE PLATFORMS

3-026 **Introduction** The obligations of online platforms are multiple and span a wide range of areas that are covered in both horizontal and sector specific EU legislation.[41] This section covers the general obligations of platforms derived from the fact that they provide information society services and which are aimed at ensuring that they operate in a transparent manner in the market in general. The section also covers the obligations that the platforms providing intermediation services and search engines have towards their business users, which ensure that they act fairly and transparently towards the many businesses that rely heavily on online platforms to offer their goods and services. Some online platforms are considered as having such market power that this could lead them to behave unilaterally and therefore unfairly towards both business users and consumers or end users in general. These regulatory rules therefore frame the behaviour of online platforms ex ante and complement measures that could be imposed ex post by application of competition law remedies.

1. General obligations applicable to online platforms providing information society services

(a) Transparency

3-027 **Transparency-Electronic Commerce Directive** The obligations on transparency of online platforms derive from the Electronic Commerce Directive and the Services Directive and are aimed at providing users in general (i.e. consumers, business users, public authorities) with general information on the service and the

[38] Electronic Commerce Directive art.3.4 (a) (i).
[39] Electronic Commerce Directive art.3(4).
[40] Commission First Report of 21 November 2003 on the application of Electronic Commerce Directive, COM(2003)702.
[41] Many of those obligations are reviewed in other chapters of this book. Also, see Edwards *Law, Policy and the Internet* (Portland/Oxford, Hart, 2017).

service provider.[42] Information society services providers must, according to the Electronic Commerce Directive, make available, in particular, their name, geographic address, details enabling rapid contact, relevant entries in trade or similar registers, and VAT number (where relevant). If the activity is subject to a specific authorisation scheme, elements to identify the competent supervisory authority should be made available.[43] Member States should also make sure that certain information is made available through national points of single contact to be set-up under the Services Directive.

Services Directive The Services Directive adds other information requirements. **3-028**
For instance, service providers in scope[44] also need to provide information on their general conditions of use, the existence of clauses on the law applicable to the contract and/or on the competent court, and on the main features of the service, if not apparent from the context.[45] The information can be made available in a number of ways, according to the provider's preference: either at the supplier's own initiative or it must be easily accessible by the recipient at the place where the service is provided. In any event, it needs to be communicated in a clear and unambiguous manner, either before the contract is concluded or if there is no contract, before the service is provided.[46] Some information also needs to be made available if the recipients of services request it. This mainly concerns the price of the services, whether or not out of court dispute settlement is possible and the application of codes of conduct.

(b) Non-discrimination

Non-discrimination under the Services Directive According to the Services **3-029**
Directive, recipients of services (i.e. consumers and businesses of the services that are in scope of the Directive) cannot be made subject to discriminatory requirements based on nationality or place of residence and the Member States must ensure that this is respected. However, it is possible to have differences in the conditions of access where these differences are directly justified by objective criteria. For instance, different tariffs and conditions could apply to the provision of a service, if this is justified because of additional costs due to the distance involved or different market conditions, such as higher or lower demand influenced by seasonality, different vacation periods or pricing by competitors.[47]

Non-discrimination under the Geo-Blocking Regulation A specific Regula- **3-030**
tion to address unjustified geo-blocking was adopted because the provision on non-discrimination of the Services Directive was not fully effective in combatting

[42] This section does not cover obligations relating to advertising.
[43] Electronic Commerce Directive art.5.
[44] The Services Directive applies to information society services but not to certain activities such as electronic communications services and networks, financial and payment services, audiovisual services, gambling activities and transport services (art.2). The Directive (art.3) also specifies that if the requirements of the Services Directive contradict requirements of more specific legislation, the requirements of the more specific legislation is applicable.
[45] Services Directive art.7.
[46] Services Directive art.7(3).
[47] Services Directive art.20 and recital 95.

discrimination and did not sufficiently reduce legal uncertainty.[48] The Regulation aims to further clarify the rule of the Services Directive by defining certain situations where different treatment based on nationality, place of residence or place of establishment cannot be justified.[49] The Regulation excludes the same services from its scope of application as the Services Directive. This means in particular that electronic communications services, transport services, audiovisual services and gambling services are excluded. It contains four main sets of rules: (i) non-discrimination in three defined situations; (ii) no blocking, limiting of access and re-routing; (iii) non-discrimination for reasons related to payment; and (iv) prohibition of passive sales.

3-031 *Non-discrimination based on country of residence or nationality in three situations* The Regulation outlaws discrimination (e.g. different pricing, refusal to sell) on the basis of nationality or place of residence when (i) the trader sells goods without delivery to the country of the customer; (ii) the trader provides electronically supplied services such as cloud services (but this does not apply if the main feature of the service is to provide access to and use of copyright protected works or other protected subject matter, including the selling of copyright protected works or protected subject matter in an intangible form);[50] or (iii) the trader provides services that are supplied in a different Member State than that of the customer (e.g. hotel booking).[51]

3-032 *Blocking, limiting access and re-routing* The Regulation prohibits traders from blocking or limiting access to their websites and apps (or other online interfaces) and from automatic re-routing based on the customer's country of residence or nationality. Re-routing is only allowed if customers explicitly consent to it (e.g. by ticking a box).[52]

3-033 *Non-discrimination for reasons related to payment* The Regulation prevents traders from applying different conditions to payment transactions based on a customer's country of residence or nationality, the location of a payment account or the place of issue of the payment card.[53]

3-034 *Prohibition of passive sales* Although the Regulation does not affect the application of competition law,[54] it reiterates that contractual restrictions that prevent a trader from responding to unsolicited requests from individual customers for the

[48] Regulation 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations 2006/2004 and 2017/2394, and Directive 2009/22 [2018] OJ L60I/1. See also Commission Staff Questions & Answers of 20 September 2018 on the Geo-blocking Regulation, available at: *https://ec.europa.eu/digital-single-market/en/news/geo-blocking-regulation-questions-and-answers* [Accessed 15 September 2019].

[49] Geo-Blocking Regulation recital 4.

[50] The review clause (art.9) of the Regulation specifies that the Commission should in its first evaluation report examine whether the regulation should be extended to cover services which provide access to copyright protected material and other subject matter.

[51] Geo-Blocking Regulation art.4(1).

[52] Geo-Blocking Regulation art.3(1.2). These practices are however allowed when blocking, limiting access or redirection is necessary to comply with a legal obligation.

[53] Geo-Blocking Regulation art.5.

[54] Those rules are explained in the Commission Guidelines of 20 April 2010 on Vertical Restraints

sale of goods without delivery, outside the trader's contractually allocated territory for reasons related to customer's nationality, place or residence or place of establishment, should be automatically void, when they impose on traders acting in breach of the prohibitions laid down in the Regulation regarding access to online interfaces, access to goods or services and payment.[55]

Cross-border portability of online services in the internal market Although not directly linked to the obligation of non-discrimination, it is worth noting that the Regulation on the cross-border portability of online content services in the internal market obliges providers of online content services offered against payment, such as Netflix, to offer to their subscribers who are temporarily present outside their country of residence the cross-border portability of the services to which they have subscribed to, at no additional cost.[56] **3-035**

(c) Electronic contracts and commercial communications

Contracts concluded by electronic means The Electronic Commerce Directive includes some key rules to make sure that contracts can be concluded electronically. First, Member States must remove legal obstacles which would prevent the use of online contracts and online contracts cannot be denied legal validity on the ground that they are formed by electronic means.[57] The Directive also lists categories of contracts which Member States could decide should not be concluded electronically. The Directive also enshrines the principle that for all contracts concluded by electronic means, and except when agreed otherwise by parties who are not consumers, the service provider needs to acknowledge receipt of the recipient's order without undue delay and electronically. The order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.[58] **3-036**

Minimum transparency Further, some minimum information requirements are imposed on service providers to ensure legal certainty and consumer confidence. The following information must be given before the placing of the order and must be available in a clear and unambiguous manner: the technical steps to follow to conclude the contract; the storage and accessibility of the concluded contract (if any); the technical means to identify and correct errors prior to the placing of the order; the languages offered to conclude the contract; and subscription to codes of conduct (if any) and any information on how to consult them electronically.[59] **3-037**

Commercial communications The Electronic Commerce Directive foresees that any form of communication that is designed to promote directly or indirectly the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession must clearly identify: the commercial communication itself; and the natural or legal person on **3-038**

[2010] OJ C130/1.

[55] Geo-Blocking Regulation art.6 and recital 34.

[56] Regulation 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market [2017] OJ L168/1, analysed in Chapter VIII of this book.

[57] Electronic Commerce Directive art.9.

[58] Electronic Commerce Directive art.11.

[59] Electronic Commerce Directive art.10.

behalf of whom the commercial communication is made. Further, promotional offers (e.g. discounts) and promotional competitions or games must also be clearly identified and there should be easy access to the conditions of participation and applicable conditions of participation.[60]

2. Additional specific obligations applicable to online platforms providing intermediation services and search engines

3-039 **Territorial scope of application** The Regulation on fair treatment of business users of online platforms imposes, from July 2020 onwards, additional transparency obligations on the providers of two specific categories of information society service: the online intermediation services ("OIS") and the online search engines. Those obligations apply in B2B relationships. Recognising the global dimension of those services, the Regulation applies regardless of where the platform is established in a Member State or outside of the European Union provided two cumulative conditions are met: (i) the business users, or the corporate website users in the case of search engines, are established in the EU; and (ii) the business users, or corporate website users, offer through the OIS/search goods or services to consumers located in the EU at least for part of the transaction. To determine if they are offering goods or services to consumers in the EU, account should be had to the fact they direct their activities to consumers located in the EU, regardless of their place of residence or nationality.[61]

(a) Additional transparency obligations applicable to intermediation services

3-040 **Requirements applicable to OIS** To ensure adequate protection of the business users of platforms, OIS providers need to make sure that their standard terms and conditions meet certain requirements, which are largely inspired by rules contained in consumer protection legislation such as in the Unfair Contract Terms Directive.[62] The Regulation also contains transparency rules on the restriction, suspension and termination of OIS, the ranking of goods and services on the platform, the offering of ancillary goods and services by the platform itself or by third parties, differentiated treatment, access to data, MFN clauses and dispute resolution.

3-041 **Standard contract terms and conditions of OIS providers** The rules to protect business users of platforms only apply if the terms and conditions governing the contractual relationship between the OIS provider and its business users have been unilaterally determined by the platform.[63] The terms and conditions must be drafted in plain and intelligible language, be easily available (including at the pre-contractual stage), must set out the grounds for suspension/termination/imposition of other restrictions, include information on other distribution channels through

[60] Electronic Commerce Directive art.6.

[61] Regulation on fair treatment of business users of online platforms art.1(2) and recital 9.

[62] Council Directive 93/13 of 5 April 1993 on unfair terms in consumer contracts OJ [1993] L95/29, reviewed in Chapter VII of this book.

[63] This is determined on the basis of an overall assessment, for which the relative size of the parties concerned, the fact that a negotiation took place, or that certain provisions thereof might have been subject to such a negotiation and determined together by the relevant provider and business user is not, in itself, decisive: art.2(10).

which the platform could market goods and services offered by the business users and include information on the ownership and control of the intellectual property rights of business users. Platforms should notify business users on a durable medium of any proposed changes to the terms and conditions and these changes cannot be implemented before the expiry of a notice period which is reasonable and proportionate. In any event the notice period cannot be less than 15 days from the date of notification of the business user. Terms and conditions which do not comply with these requirements are null and void. Further, platforms need to make sure that the identity of business users providing goods or services is clearly visible on the platform.[64] To make sure the contractual relations are fair, OIS cannot impose retroactive changes to terms and conditions (except when they are required to respect legal obligations or when the changes benefit the business users) and they must ensure that the terms and conditions include information on the conditions under which businesses can terminate the agreement.[65]

3-042 **Restriction, suspension and termination of OIS** If the platform wants to restrict or suspend the OIS in relation to a given business user, it must inform the business user of the reasons for that decision on a durable medium.[66] If the platform wants to terminate the OIS in relation to a given business user, it should normally have to give a statement of reasons at least 30 days before the termination takes effect. In all cases (restriction, suspension or termination) the business user must be given the opportunity to resort to an internal complaints handling procedure.[67]

3-043 **Ranking of goods or services** Platforms should set out in their terms and conditions the main parameters determining ranking and the reasons justifying the weighting of a given parameter relative to another. If remuneration influences ranking, the platform must also set this out together with the effects of payment on the ranking. In any event, platforms do not need to disclose algorithms.[68]

3-044 **Ancillary goods or services** If ancillary services or goods are offered either by the platform itself or by a third party (such as financial products), the platform must set out in the terms and conditions a description of the type of products and services and of the extent to which the business user is allowed to offer his own ancillary services/goods through the platform.[69]

3-045 **Non-discrimination** The terms and conditions of OIS should include a description of any differentiated treatment the platform may give in relation to goods and services offered to consumers by either the platform itself (or by another business user which the platform controls) and other business users. This differentiated treatment could be linked to access to personal data or other data, ranking or other set-

[64] Regulation on fair treatment of business users of online platforms art.3.

[65] Regulation on fair treatment of business users of online platforms art.8(a) and (b).

[66] Regulation on fair treatment of business users of online platforms art.4. The statement of reasons must be given to the business user before or at the time the restriction/suspension takes effect.

[67] Regulation on fair treatment of business users of online platforms art.4(3).

[68] Regulation on fair treatment of business users of online platforms art.5. The Commission has to publish guidelines on these transparency requirements.

[69] Regulation on fair treatment of business users of online platforms art.6. Ancillary services are defined as goods or services offered to the consumer before the completion of the transaction initiated on the OIS in addition to and complementary to the primary good or service offered by the business user through the OIS: Regulation on fair treatment of business users of online platforms art.2(11).

tings; direct or indirect remuneration charge for the use of the service, or access or conditions for any remuneration charged for the use of services, functionalities or technical interfaces that are relevant to the business user using the platform.

3-046 **Access to data** Personal data and other data such as ratings and reviews are extremely valuable in the platform economy. Although the Regulation does not oblige any form of access or sharing, it does impose on OIS providers an obligation to be transparent towards business users on the access and sharing arrangements relating to data.[70] The terms and conditions must contain a description of the conditions of access (or absence thereof) by business users to personal data or other data which the business users themselves or the consumers provide for the use of the OIS or which are generated through the provision of the service. Platforms should in particular inform business users of whether the platform also has access to this data, under which conditions and in addition, whether any data is provided to third parties. If the sharing of data is not necessary, platforms should provide the reasons for sharing the data and any scope for the business user to opt out from the data sharing.[71]

3-047 **Most favoured nation (MFN) clause** Finally, where platforms restrict the ability of business users to offer the same products to consumers through other channels under different conditions, the grounds for such restrictions should be included in the terms and conditions and make sure the grounds are easily available to the public.

(b) Additional transparency obligations applicable to online search engines

3-048 **Requirements applicable to search engines** The specific transparency rules on ranking and on differentiated treatment also apply to online search engines, while the other rules only cover OIS. On ranking, search engines should make publicly available on the search engine a description in plain and intelligible language of the most significant parameters that determine ranking and the relative importance of those main parameters. Where payment influences ranking, this should also be clearly specified. Corporate website users should be given the possibility to inspect the contents of a notification received by the search engine which has led to the altering of a ranking order. Algorithms should however not be disclosed.[72] Search engines should set out a description of any differentiated treatment they may give in relation to goods or services offered to consumers.[73]

D. LIABILITY OF ONLINE PLATFORMS

3-049 **Need of a particular liability regime for online platforms** The arrival of new communications technologies at the turn of the century made traditional content regulation problematic, unfeasible and impractical in the context of the Internet.

[70] Processing of personal data should however comply with the applicable legislative framework and in particular the General Data Protection Regulation 2016/679 (GDPR) reviewed in Chapter V of this book.

[71] Regulation on fair treatment of business users of online platforms art.9.

[72] Regulation on fair treatment of business users of online platforms art.5(2) to (7).

[73] Regulation on fair treatment of business users of online platforms art.7(2) and (3).

Removal of technical and geographical boundaries democratised the flow of information but proved challenging for regulators, litigants and the creative industries. Yet, the first to decide on issues of intermediary liability were judges, not the legislature.[74] From the late 1990s, when the internet became popular among the general public, courts across the EU held service providers liable for their users' information.[75] The first wave of lawsuits ran counter to efforts to popularise and facilitate e-commerce and endangered the development of the internet and the web generally.[76] Legislators, however, found it inappropriate to apply the traditional liability criteria to intermediaries' activities considering the volumes of information that they process. The ensuing legal uncertainty led legislatures around the world to enact specific rules about the legal responsibility of internet intermediaries.[77]

1. General liability regime

(a) Liability exemption for providers of intermediary services

3-050 **Liability exemptions for intermediaries** The Directive on electronic commerce regulates the liability of intermediary service providers. This part of the Directive contains provisions introducing EU liability exemptions for certain types of intermediary services. Only three types of services are covered, namely "mere conduit" (art.12), "caching", (art.13) and "hosting" (art.14). In order to benefit from these exemptions, providers of such services must comply with the conditions of each article. If the conditions for being exempt from liability are not met, this does not mean that the intermediary is automatically liable. The effect is that the intermediary can no longer rely on the EU immunity. The question of liability is then determined under the applicable material law specific to the type of infringing content in each Member State (e.g. copyright law or anti-defamation law). Questions concerning liability or injunctions must be assessed by taking into account the specific service in question.[78]

3-051 **Rationale and functional scope** The liability provisions of the Directive on electronic commerce reconciled the two main arguments of the debate taking place

[74] Stalla-Bourdillon, "Internet intermediaries as responsible actors? Why it is time to rethink the e-Commerce Directive as well", in Floridi and Taddeo, *The Responsibilities of Online Service Providers* (Springer, 2016).

[75] Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach" (2011) 48 *Common Market Law Review* 1455–1502, p.1455.

[76] e.g. in Germany, Felix Somm, the general manager of CompuServe Germany, was prosecuted for facilitating access to violent and child sexual abuse material stored in newsgroups accessible by CompuServe's customers; in Belgium, the Commercial Court of Brussels issued an injunction against hosting provider Skynet for storing illegal MP3 files; in the UK, internet access provider Demon was held liable for defamatory statements uploaded by one of its users.

[77] Van Hoboken, *Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines* (Alphen aan den Rijn, Kluwer Law International, 2012).

[78] Husovec, *Injunctions Against Intermediaries in the European Union—Accountable But Not Liable?* (Cambridge, Cambridge University Press, 2017) p.12 defining "an injunction" as a court order by which an individual is required to perform, or is restrained from performing a particular act (for instance provide information, implement technical features, refrain from providing service to somebody).

between the internet industry and EU policy makers at the time.[79] On the one hand, there was the concern that if intermediaries were to be held liable for third party content on similar grounds as "publishers", this could restrain service providers from entering the market. On the other hand, the Commission recognised the role that online intermediaries could play in limiting illegal online content and, through that, improve public trust and confidence in the internet as a safe space for economic activity. The balance that was reached was meant to stimulate growth and innovation of the newly born technology and provide positive incentives for further development.[80] The scope of the liability exemptions is horizontal. This means that the liability exemptions cover various types of illegal content and activities (defamation, content harmful to minors, unfair commercial practices, etc.) and different kinds of liability (criminal, civil, direct, indirect, etc.).[81] The protection of the Directive is situated at the service level, and not at the company level. Therefore, a single company can at the same time act as a mere conduit, caching and/or hosting provider.

(b) Mere conduit and caching services

3-052 **Mere conduit** Article 12 targets traditional infrastructure operators and internet access providers. The liability exemption refers to providers of "mere conduit" services described as services which consist of the transmission in a communication network of information provided by a recipient of the service (transmission services) and services which consist of the provision of access to a communication network (access services). Recital 42 further stipulates that the exemptions provided by the Directive apply only to cases "where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network". It further elaborates that such activities are of a mere technical, automatic, and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information it transmits or stores. While recital 42 purports to address all of the exemptions of the Directive, one might argue that the scope of this part of the recital should be limited to the transmission and access services identified in arts 12 and 13, which address access and transmission services.[82] The services described in art.12 are sometimes compared to postal services, which are similarly not held liable for the illegal content of a letter.

3-053 *Extension* The liability exemption for mere conduit extends to the automatic, intermediate and transient storage of the information transmitted. This is the case if the storage takes place for the sole purpose of carrying out the transmission in

[79] OECD, *The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy* (2011) Pt II, p.12.

[80] Electronic Commerce Directive recitals 1 to 6.

[81] Helberger et al., "Legal Aspects of User Created Content" in IDATE, TNO, IViR, User-Created Content: *Supporting a Participative Information Society* (Study for the European Commission, 2008), available at: *http://www.ivir.nl/publications/helberger/User_created_content.pdf* [Accessed 12 September 2019], p.220.

[82] Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach" (2011) 48 *Common Market Law Review*; Montéro, "Les responsabilités liées au web 2.0" (2008) 32 *Revue du Droit des Technologies de l'Information* 367.

the communication network. Moreover, the information cannot be stored for any period longer than is reasonably necessary for the transmission.[83]

Conditions of application The mere conduit exemption of liability only applies on the condition that the service provider: (i) does not initiate the transfer of data; (ii) does not select the recipient of the data; and (iii) does not select or modify the transmitted data. Despite the lack of liability of the service provider (when the conditions are met), national courts and administrative authorities may direct prohibitory injunctions towards a provider of a mere conduit service. Such injunctions must be in accordance with the law of the Member State where the case is adjudicated.[84] **3-054**

Caching "Caching" is defined as: **3-055**

> "...the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request."[85]

Article 13 is targeted at providers of so-called "proxy-servers", which store local copies of websites to speed up the subsequent consultation of these websites by other customers. The exemption covers only information society services that consist of the transmission in a communication network of information provided by a recipient of the service (transmission services).[86] Just as mere conduits, providers of this type of service can only be exempted from liability if they are in no way involved with the information transmitted.[87]

Conditions of application In addition, the following five conditions must be met in order for a service provider to benefit from the caching exemption[88]: service providers (i) may not modify the information as it would deprive them of the position of the intermediary; (ii) have to comply with conditions on access to the information; (iii) must update the information regularly in accordance with the generally recognised rules and practices in this area; (iv) may not interfere with the lawful use of technology that is used to measure the use of information; and (v) must remove the cached information immediately upon obtaining actual knowledge that the initial source of the information is removed, access to it has been disabled, or that a court administrative authority has ordered such removal or disablement. The liability exemption for caching does not affect the power of courts or **3-056**

[83] Electronic Commerce Directive art.12(2).

[84] Electronic Commerce Directive art.12(3). See *UPC Telekabel Wien* (C–314/12), EU:C:2014:192 addressing an injunction towards an internet service provider to block access of its customers to a website making copyright infringing materials available to the public.

[85] Electronic Commerce Directive art.13(1).

[86] Electronic Commerce Directive art.13(1). When comparing the caching exemption with the exemption for transient storage under the "mere conduit" rule of art.12(2), the wording appears to be very similar. The key difference between the caching exemption for transient storage and the exemption for transient storage under the mere conduit provision therefore is the purpose for which the storage is taking place: Lodder, "Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market", in Lodder and Kasspersen (eds), *eDirectives: Guide to European Union Law on E-commerce—Article by Article Comments* (Alphen aan den Rijn, Kluwer Law international, 2002), p.88.

[87] Electronic Commerce Directive recital 43.

[88] Electronic Commerce Directive art.13(1).

administrative authorities to issue prohibitory injunctions in accordance with the national legal system.[89] So far, art.13 is rarely the subject of litigation.

(c) Hosting services

3-057 **Definition** Article 14 of the Directive on electronic commerce provides a liability exemption for hosting service providers, that is, information society services consisting of the storage of information provided by a recipient of the service at his request.[90] Typically, it concerns webhosting services that provide web space to their users, where users can upload content to be published on a website. However, numerous other services also fall within the scope of hosting services and the precise extent of its scope is a subject of discussion. The storage by "hosting" service providers differs from the storage carried out in the context of mere conduit or caching, mainly in terms of the purposes for which the storage takes place. In contrast to mere conduit or caching services, hosting storage is not merely "incidental" to the provision of the transmission or access services.[91] Storage may be provided for a prolonged period of time, and may also be the primary object of the service.[92]

3-058 *Neutrality requirement* The Court of Justice specified in *Google France* that to enjoy the benefit of the liability exemption, a service provider's conduct must be neutral. The Court defined neutrality as a conduct that is "technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores".[93]

3-059 *Knowledge requirement* However, in *L'Oréal v eBay*, the Court of Justice seemingly reduced the standard by replacing the "neutrality" requirement with "lack of knowledge". The Court ruled that art.14 of the Directive applies to hosting providers if they do not play an active role that would allow them to have knowledge or control of the stored data.[94] The requirement that an intermediary's activities are of a mere technical, automatic and passive nature is based on recital 42 of the Directive. These properties of the service imply that the intermediary has neither knowledge of, nor control over the information it transmits or stores. The wording of the recital, however, is problematic. While it purports to address all of the exemptions of the Directive, some argue that the scope of this recital should be limited to the transmission and access services identified in arts 12 (mere conduit) and 13 (caching). As is further clarified in recital 43, not being involved in any way with the transmitted information is actually a condition for liability exemption for mere

[89] Electronic Commerce Directive art.13(2).

[90] For a recent analysis of the scope of art.14 in the light of the developments in the online landscape, see van Hoboken, Quintais, Poort and van Eijk, *Hosting intermediary service and illegal content online* (2018, Study for the European Commission).

[91] Walden, Cool, and Montero, "Directive 2000/31/EC—Directive on electronic commerce", in Bullesbach, Poullet and Prins (eds), *Concise European IT Law* (Alphen aan den Rijn, Kluwer Law International, 2005), p.253.

[92] This exemption was originally aimed at ISPs providing space on their internet servers for third parties' websites, or bulletin boards or chat room services provided by the ISP itself—where the ISP only provides technical means for the users' communication without interfering with the content being communicated between the user, see Jakobsen "Mobile Commerce and ISP Liability in the EU" (2010) 19 *International Journal of Law and Information Technology*, p.44.

[93] *Google France and Google v Louis Vuitton a.o.* (C–236/08 to C-238/08) EU:C:2010:159, paras 113 to 114.

[94] *L'Oréal v eBay* (C–324/09) EU:C:2011:474, paras 112 to 116.

conduit and caching services. The exemption for hosting in art.14 of the Directive is not limited in scope to either transmission or access services. According to Van Eecke, art.14 in fact does not require a passive role of the hosting provider in order for the protection regime to apply.[95] A hosting provider can still be protected even if it is not completely passive—as long as it does not have knowledge or control over the data that is being stored. This approach is referred to as "storage but no knowledge" test. Following this line of reasoning, active intermediaries could still benefit from the safe harbour offered by the Directive on electronic commerce, provided that they do not have knowledge or control over the data that is being stored.

3-060 **Extended scope of application** The exemptions provided by the Directive are defined in functional terms (i.e. in terms of the activity being performed), not in terms of the qualification of the actor. While the European legislator arguably only envisioned providers whose services consisted mainly, if not exclusively, of the performance of operations of a strictly technical nature, the scope of the exemption may also be applied to other entities—provided that the conditions set forth by art.14 are met. As a result, the exemption may in principle benefit any type of service provider who stores content at the request of the recipient; including so-called "web 2.0" service providers.[96]

3-061 **Conditions of application** A hosting service provider is liable for the information stored, on the condition that the provider (i) is not aware of the facts or circumstances from which the illegal activity or information is apparent—with regard to civil claims for damages, and he does not have actual knowledge of the illegal activity or information—with regard to other claims; or (ii) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[97]

3-062 *Level of knowledge* The Directive introduces different levels of knowledge with regard to criminal and civil liability. For the former, "actual knowledge" is required, while for the latter it is enough to establish "constructive knowledge" of the service provider. This means that, as regards claims for damages, the service provider may be found liable where it is "aware of facts or circumstances from which the illegal activity or information is apparent".[98] Upon obtaining such knowledge or awareness, the service provider has to act expeditiously to remove, or disable access to, the information. Apparent illegality occurs, according to the Court of Justice in *L'Oréal v eBay*, when "any diligent economic operator should have identified the illegality in question".[99] Such "constructive knowledge" covers every situation in which the provider concerned becomes aware, in one way or another, of such facts

[95] Van Eecke, "Online Service Providers and Liability: a Plea for a Balanced Approach" (2011) 48 *Common Market Law Review* 1455–1502, p.1463.

[96] See Montéro, "Les responsabilités liées au web 2.0" (2008) 32 *Revue du Droit des Technologies de l'Information* 367.

[97] Electronic Commerce Directive art.14(1).

[98] Kaspersen and Lodder (eds) *eDirectives: guide to European Union law on e-commerce: commentary on the directives on distance selling, electronics signatures, electronic commerce, copyright in the information society, and data protection* (The Hague/New York, Kluwer, 2002), pp.88–89. This distinction, however, has not been transposed into all national legislations.

[99] *L'Oréal v eBay* (C–324/09) EU:C:2011:474, para.120.

or circumstances.[100] In particular, it covers both the situation where the operator of an online marketplace uncovers an illegal activity or illegal information as result of an investigation undertaken on its own initiative, and the situation where the operator is notified by a third party. Such notification represents, as a general rule, a factor indicating "awareness", although it could turn out to be insufficiently precise or inadequately substantiated. Requirements for valid notification, as well as interpretations of actual and constructive knowledge, differ across EU countries. For example, the interpretations of "actual knowledge" range among the EU countries from knowledge obtained through a court order, to informal notice by a user, which, however, should be sufficiently substantiated.[101] Divergent case law across the EU shows that there is a lack of consistency in the interpretation of these terms and the ensuing requirements for a valid notice.[102]

3-063 **Exception** The exemption of art.14 does not apply when the recipient of the service is acting under the authority or the control of the provider.[103] For example, if the service provider is acting as an employer or supervisor of the service recipient, it does not qualify for the exemption if the content was introduced pursuant to its instructions. Similarly, as in the case of the mere conduit and caching services, the liability exemption does not affect the possibility of a court or administrative authority, in accordance with Member States' regulations, requiring the service provider to terminate or prevent an infringement.[104]

3-064 **Notice and takedown** Moreover, Member States may establish specific procedures governing the removal or disabling of access to information. The Directive does not clarify any details for taking down or blocking access to content. As a result, there are no guidelines on how such processes should be handled by service providers, nor safeguards to ensure proportionality or due process. Procedural aspects were left entirely to the discretion of the Member States.[105] Some EU countries have provided a more detailed regulation for the hosting exemption by introducing formal notification procedures. Many, however, opted for a verbatim transposition of the Directive, leaving, therefore, this matter unresolved.[106]

(d) Monitoring

3-065 **No general obligation to monitor** Member States may not impose on providers of mere conduit, caching or hosting services a general obligation to monitor information they transmit or store.[107] Also, Member States cannot introduce a general obligation to actively look for facts or circumstances indicating illegal

[100] *L'Oréal v eBay* (C–324/09) EU:C:2011:474, para.121.
[101] *L'Oréal v eBay* (C–324/09) EU:C:2011:474, para.122
[102] See for example: BGH, 23/09/2003, VI ZR 335/02; Dutch Supreme Court 25 November 2005, LJN Number AU4019, Case Number C04/234HR; Turner and Levat, "The Spanish Supreme Court clarifies the concept of actual knowledge in connection with ISP's liability" (2010) 26 *Computer Law & Security Review* 440.
[103] Electronic Commerce Directive art.14(2).
[104] Electronic Commerce Directive art.14(3).
[105] Electronic Commerce Directive art.14(3). Such a delegation can be seen also in recital 46, which stipulates that the removal or disabling of access should be undertaken in observance of the right to freedom of expression and of procedures established for this purpose at national level.
[106] Commission First Report on the Application of the Directive on Electronic Commerce, COM(2003)702.
[107] Electronic Commerce Directive art.15.

activity. An obligation to conduct general monitoring of content, if permitted, would counteract the limited liability paradigm. This is because intermediary service providers actively seeking illegal activities would no longer be neutral and passive in nature, and would not be able to claim lack of knowledge. Moreover, a general monitoring obligation could lead to censorship and consequently have a negative impact on freedom of expression.[108]

Exceptions The prohibition towards monitoring obligations refers solely to monitoring of a general nature. It does not concern monitoring obligations in a specific case, nor does it affect orders by national authorities in line with national legislation.[109] The Directive also allows Member States to require hosting providers to apply duties of care, which can reasonably be expected from them.[110] Such duties of care, however, should only be introduced to detect and prevent certain types of illegal activities, foreseen by national law. To the confusion of many, the Directive does not specify what exactly such duties of care entail. As a result, the boundary between such duties and general monitoring is not clear.[111] 3-066

Case-law clarifications Article 15 of the E-Commerce Directive was a subject of two important judgments. Both cases involved *Sabam*—the Belgian rights' management company, which requested installation of filtering mechanisms to prevent copyright infringements.[112] In the first case, *Scarlett Extended*, the request was directed to an ISP provider and in the second case, *Sabam v Netlog*, to a hosting service provider—a social networking site. The requested mechanism was intended to apply to all information, by all users, as a preventive measure, for an unlimited period of time and exclusively at the expense of the service providers. The Court of Justice considered that such a measure would amount to general monitoring, which is prohibited by art.15 of the Directive.[113] Filtering of content is also the subject of the recent judgement by the Supreme Court of Austria on the scope of art.15 of the E-Commerce Directive and the host provider privilege.[114] This time, however, the case concerned hate speech and defamatory content. Specifically, the Austrian court requested clarification on a possibility of an injunction to remove specific information but also other information that is identical in wording or not identical in wording but similar in meaning. The case required balancing between the rights to privacy (due to the personal data processing that the automatic filter- 3-067

[108] OECD, *The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy* (2011) Pt II, p.36. Also Council of Europe Human rights guidelines of July 2008 for Internet Service Providers, available at *https://rm.coe.int/16805a39d5* [Accessed 13 September 2019], p.3.
[109] Electronic Commerce Directive recital 47. The application of art.15 differs across the EU in case of injunctions. For example, in Germany a host may still be required to actively monitor his platform for further infringing activity. See more in Verbiest, Spindler, et al., *Liability of Internet Intermediaries –General trends in Europe* (Luxembourg, Study for the European Commission, 2007), p.85.
[110] Electronic Commerce Directive recital 48.
[111] See more in Valcke, Kuczerawy and Ombelet, "Did the Romans Get it Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common", in Floridi and Taddeo (eds), *The Responsibilities of Online Service Providers* (Springer, 2016). Some authors even consider recital 48 as contradictory to art.15: Barceló and Koelman, "Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough" (2000) 4 *Computer Law & Security Report* 232.
[112] *Scarlet Extended v SABAM* (C–70/10), EU:C:2011:771 and *SABAM v Netlog* (C–360/10), EU:C:2012:85.
[113] *SABAM v Netlog* (C–360/10), EU:C:2012:85, para.38.
[114] *Eva Glawischnig-Piesczek v Facebook Ireland* (C–18/18) EU:C:2019:458.

ing would require), freedom of expression and freedom to conduct a business on the one hand, and combating hate speech on the other. Moreover, the Court of Justice decided that the Electronic Commerce Directive, in particular art.15, does not preclude a national court from ordering a host provider to remove information, the content of which is identifical or equivalent to the content of information previously declared to be unlawful. However, "the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content".

3-068 **Voluntary monitoring** The prohibition of art.15 is addressed to the Member States' legislators. They are not allowed to introduce regulations that would require providers of the specified services to monitor the information they store or transmit. This does not mean that service providers cannot take up such activities on their own. The prohibition should not be read as a prohibition against service providers monitoring information. Most of the online platforms do perform certain monitoring activities to maintain a "civilised" environment on their service. Voluntary monitoring, however, can prove detrimental. Exercising too much control could compromise the neutral status of the intermediary and, in consequence, deprive them of the safe harbour protection. The EU intermediary regime does not contain a provision which protects intermediaries from liability should their voluntary monitoring prove imperfect (such as the one offered by s.230(c)(2) of the Content and Decency Act ("CDA") in the US). As a result, service providers are careful not to shoot themselves in the foot through their own overzealous activities.[115]

3-069 **Cooperation with authorities** Article 15(2) defines two additional obligations that Member States may impose upon information society service providers. Firstly, Member States may require service providers to inform authorities about any alleged illegal activities of their users. Such notification needs to be given as soon as the provider becomes aware of the illegal activity. Secondly, Member States may establish obligations on providers to disclose the identity of users with whom they have storage agreements. Establishing these obligations is not a requirement and is left to the discretion of the Member States.[116]

2. Evolution of the general liability regime

3-070 **Review after 10 years** A decade after the adoption of the Directive on electronic commerce, in 2010, the Commission launched a public consultation as part of its periodic review process. The consultation revealed that the majority of respondents

[115] See Valcke, Kuczerawy and Ombelet, "Did the Romans Get it Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common", in Floridi and Taddeo (eds), *The Responsibilities of Online Service Providers* (Springer, 2016), p.114.

[116] The possibility of introducing an obligation to disclose the identity of recipients was questioned in *Promusicae v Telefonica de Espana* (C–275/06) EU:C:2008:54. See more: Coudert and Werkers, "In The Aftermath of the Promusicae Case: How to Strike the Balance?" (2010) 18 *International Journal of Law and Information Technology* 50–71.

generally did not see a need for a revision of the Directive at that stage.[117] Many respondents, however, identified the need to clarify certain aspects of the Directive, particularly with regard to intermediary liability for third-party content. The most difficult issue was the functioning of the notice-and-takedown procedures. The public consultation revealed that a number of problems with regard to such procedures persisted. Most of the stakeholders mentioned legal uncertainty as an issue, highlighting that several key terms remain subject to divergent interpretations—not only across Europe but also among different stakeholders. Rightholders generally complained about the time during which illegal content stays online, while civil society pointed out that often legal content is taken down without good reason. Many stakeholders felt that the current approach incentivises unnecessary and undesirable restrictions on the freedom of expression. The Commission concluded that procedures aimed at eliminating illegal online content should lead to a quicker takedown, but at the same time should better respect fundamental rights—in particular the freedom of expression—and should increase legal certainty for online intermediaries. Based on these findings, the Commission decided in 2011 to focus its efforts on developing a new European framework for notice and action without coming, however, with concrete actions.[118]

3-071 **Review after 20 years** Today, 20 years after the Commission proposed the Directive on electronic commerce, online platforms play a very important economic and societal role that should bring wider responsibility. This has led some Member States to adopt specific legislation to increase the liability, or at least the responsibility and the accountability, of some online platforms at the risk of undermining the Digital Single Market. This has also led the courts of some Member States to interpret the national provisions transposing the Directive in a more restrictive way, possibly increasing the divergences across national case-law which, in turn, may also undermine the Digital Single Market and legal certainty.[119] The increasing importance of online platforms and the new risks of Digital Single Market fragmentation led the Commission to pursue a three-pronged strategy:[120] (i) give more guidance on the interpretation of the controversial provisions of the Directive, in particular regarding the notice and takedown and the reliance on voluntary proactive measures; (ii) adapt sectoral hard-law when there is a specific problem; and (iii) encourage coordinated EU-wide co and self-regulation for the illegal materials which are particularly harmful. For the near future, the Commission announced the proposal of a new Digital Services Act in order to upgrade the liability and safety rules for digital platforms, services and products.

[117] European Commission, Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the Implementation of the Directive on electronic commerce (2000/31/EC), available at: *http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf* [Accessed 13 September 2019].

[118] Communication of the Commission of 11 January 2012, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, SEC(2011)1640.

[119] Kohl "The rise and rise of online intermediaries in the governance of the Internet and beyond—connectivity intermediaries" (2012) 26 *International Review of Law, Computers and Technology* 185–210; Commission Staff Working Document of 10 May 2017 on Mid-term review of DSM Strategy, SWD(2017)155, pp.28–29.

[120] Commission Communication on online platforms, COM(2016)288, p.9.

(a) Commission Communication of September 2017

3-072 **Goals of the Guidelines** In 2017, the Commission issued a Communication, under the apt title "Towards an enhanced responsibility of online platforms".[121] The Communication aims to (i) lay down a set of guidelines and principles for online platforms to step up the fight against illegal online content in cooperation with national authorities, Member States and other relevant stakeholders; (ii) facilitate and intensify the implementation of good practices for preventing, detecting, removing and disabling access to illegal content with a goal to ensuring the effective removal of illegal content, increased transparency and the protection of fundamental rights online; and (iii) provide clarifications to platforms on their liability when they take proactive steps to detect, remove or disable access to illegal content (the so-called "Good Samaritan" actions).[122] The guidelines and principles provided in the Communication, however, not only target the detection and removal of illegal content but they also seek to address concerns in relation to over-removal of legal content.[123]

3-073 **Detecting illegal content** Illegal content can be detected thanks to public authorities and courts, users or the platforms themselves when monitoring their traffic. The Communication encourages each of those channels by reminding the platforms of their obligations to cooperate with public authorities and courts, encouraging the platforms to facilitate notices by users in particular by trusted flaggers, and stimulating the reliance on voluntary proactive measures. The Communication proposes that criteria to ensure a high quality of notices and faster removal of illegal content should be agreed by the industry at EU level. Such criteria should be based on respect for fundamental rights and of democratic values.[124] The Communication continuously emphasises, moreover, that the suggested measures and safeguards should be taken "voluntarily".

3-074 *Good Samaritan* Interestingly, the Communication encourages proactive content moderation and aims to clarify intermediaries' liability in such circumstances. Specifically, the Commission argues that taking such voluntary, proactive measures does not automatically lead to the online platform losing the benefit of the liability exemption.[125] With this reading, the Commission seems to advocate for a "European version" of the Good Samaritan protection. Proactive measures taken by an intermediary to detect and remove illegal content may indeed result in obtaining knowledge or awareness of illegal activities or illegal information, which could lead to the loss of the liability exemption. However, the Commission argues that in such cases, the intermediary:

[121] Communication of the Commission of 28 September 2017, Tackling Illegal Content Online—Towards an enhanced responsibility of online platforms, Brussels, COM(2017)555.

[122] Communication of the Commission of 28 September 2017, Tackling Illegal Content Online—Towards an enhanced responsibility of online platforms, Brussels, COM(2017)555, p.3.

[123] Communication of the Commission of 28 September 2017, Tackling Illegal Content Online—Towards an enhanced responsibility of online platforms, Brussels, COM(2017)555, p.6.

[124] Communication of the Commission of 28 September 2017, Tackling Illegal Content Online—Towards an enhanced responsibility of online platforms, Brussels, COM(2017)555, p.6.

[125] Communication of the Commission of 28 September 2017, Tackling Illegal Content Online—Towards an enhanced responsibility of online platforms, Brussels, COM(2017)555, p.10. This was already the line taken by the Commission in its Communication on the collaborative economy, COM(2016)356, p.9.

"...continues to have the possibility to act expeditiously to remove or to disable access to the information in question upon obtaining such knowledge or awareness."[126]

If the intermediary does so, he continues to benefit from the liability exemption. Therefore, the intermediary should not be concerned about implementing proactive voluntary measures.

3-075 *Confusing interpretation* The presented interpretation of art.14 of the Directive is interesting, but somewhat confusing and perhaps even misleading. Specifically, the Commission argues that intermediaries should not worry about losing immunity because under art.14 they already have an obligation to act expeditiously when they obtain knowledge or awareness. This includes situations when the knowledge or awareness is obtained "as the result of an investigation undertaken on its own initiative".[127] The fact that intermediaries can "choose" whether they comply with that obligation to maintain the immunity, according to the Commission, is equivalent to the continuous benefit from the liability exemption. Arguably, this is the case under the assumption that they always "choose" to remove or block access. In other words, the Commission attempts to convince intermediaries that they do not lose the protection—as long as they act according to the expectations of policy makers. However, the conditional character of the immunity is omitted in that argumentation. Moreover, the Commission overlooks the difference in scale between the situation when intermediaries stumble upon illegal content occasionally, and when they would regularly find illegal content as a result of using proactive measures. After all, the more intermediaries look, the more they will find. The chances of missing a particular instance of illegality, and therefore losing the immunity, grow significantly with increased searching.

3-076 *EU-US difference* In any event, the proposed interpretation is not a Good Samaritan protection in the meaning of s.230 of the US CDA. This is because s.230 CDA protects intermediaries when they take any voluntarily measure to restrict access to or availability of certain content but also, and most importantly, when they miss such content and do not take any action at all. After all, the specific purpose for introducing this section was to overrule the judgment of *Stratton-Oakmont v Prodigy*, which found internet service provider, Prodigy, liable for defamatory comments made by an unknown user on one of its bulletin boards.[128] The court ruled that Prodigy was a "publisher" and therefore liable for the statements; if, in the alternative Prodigy had been found to only be a "distributor" of the information, this would have absolved it of liability. The judgment turned on the significant editorial control exercised by Prodigy, due in part to its editorial staff who had the ability to continually monitor incoming transmissions. On the basis of the judgment, the more measures internet service providers implemented to monitor content on their websites, the more likely they were to be held liable for the nature of such content. By providing the assurance under s.230 CDA, the US Congress effectively encouraged intermediaries to implement such proactive measures, without

[126] Communication of the Commission of 28 September 2017, Tackling Illegal Content Online—Towards an enhanced responsibility of online platforms, Brussels, COM(2017)555, p.12.

[127] *L'Oréal v eBay* (C–324/09) EU:C:2011:474, paras 120 to 121.

[128] *Stratton Oakmont v Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). See more in Keats Citron and Wittes "The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity" (2017) *University of Maryland Francis King Carey School of Law, Legal Studies Research Paper* 2017–22, p.4.

the negative consequences of *Stratton-Oakmont v Prodigy*. In contrast, the Commission's argumentation is actually only half of the Good Samaritan protection—intermediaries in the EU will not lose the immunity if they take voluntary action, but there is no protection if they fail to do so.

3-077 **Removing illegal content** Once illegal content has been identified, the platforms should remove it. The Communication reminds the platforms that they should act expeditiously which, in practice, depends on the type of illegal content, the accuracy of the notice and the potential damage caused. Platforms should enhance transparency on their content policy and their notice-and-takedown procedures. They should also allow counter-notice to alleviate over-removal and abuse of the system. The Communication presents a number of safeguards for free expression in content removal mechanisms, for example it proposes the introduction of a counter-notice mechanism, and promotes redress mechanisms, transparency and accountability.

3-078 **Content stay-down** Regarding the prevention of re-appearance of illegal content, the Communication encourages platforms to take measures which dissuade users from repeatedly uploading illegal content of the same nature and to develop and use automated technologies in that regard.

(b) Commission Recommendation of March 2018

3-079 **Goals of the Recommendation** As a follow-up to the Communication of 2017, the Commission adopted in March 2018 a Recommendation on measures to effectively tackle illegal content online.[129] The Recommendation aims to guide the activities of the Member States and the online platforms in effectively tackling illegal content online and to safeguard the balanced approach that the Directive on electronic commerce seeks to ensure. The Recommendation highlights, again, that intermediaries have particular societal responsibilities to help tackle illegal content disseminated through the use of their services. Those responsibilities imply that the intermediaries should be able to make swift decisions regarding possible actions with respect to illegal content online, and that they should put in place effective and appropriate safeguards. Overall, however, the Recommendation appears to take a more nuanced approach than the Communication. The recommendations provided are directed to both Member States and the intermediaries.[130] The instrument provides general recommendations applicable to all types of illegal content and specific recommendations relating to terrorist content.

3-080 **Notice and takedown** The general section recommends the introduction of mechanisms to submit notices.[131] Those mechanisms should be easy to access, user-friendly and allow for the submission of notices by electronic means. They should also encourage the submission of notices which are sufficiently precise and

[129] Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online [2018] OJ L63/50.

[130] Although the Recommendations are not binding according to art.288 TFEU, national authorities and courts have to take them into consideration, in particular when they cast light on the interpretation of EU law: *KPN v Autoriteit Consument en Markt (ACM)* (C–28/15) EU:C:2015:610, para.42 and case-law quoted; see para.2-062 of this book.

[131] Commission Recommendation 2018/334 on measures to effectively tackle illegal content online, paras 5 to 8.

adequately substantiated, to facilitate the decision-making process by the service providers. The Recommendation, moreover, specifies that notice providers should have the possibility, but not be required, to include their contact details in a notice to allow the online platform to ask for additional information or inform the notice provider about any intended follow-up. The Recommendation suggests that content providers should, as a matter of principle, be informed of the decision to remove or disable access to their content. Such notifications help to ensure transparency and fairness and avoid the unintended removal of content that is not illegal content. Moreover, the content provider should be allowed to file a counter-notification.[132] The ability to file a counter-notification enables content providers to contest the decision on removal or disabling access to their content. Hosting service providers should take due account of any counter-notice that they receive. The Recommendation specifies, importantly, that where the information in counter-notification indicates the content is not illegal, the hosting provider should reverse its decision to remove or disable access without undue delay.

3-081 **Proactive measures** The Recommendation follows the steps of the Communication by encouraging the use of proactive measures.[133] Specifically, the Commission argues that it can be appropriate to take such measures where the illegal character of the content has already been established or where the type of content is such that contextualisation is not essential. The Commission, therefore, has not revised its position presented in the Communication and does not consider that using automatic detection tools would lead to a loss of immunity by making hosts active. The Recommendation highlights the importance of safeguards, to avoid removal of content that is not illegal. Such safeguards should consist, in particular, of human oversight and verifications, and should be applied, in particular, in relation to the use of automated means to avoid any unintended and erroneous decisions. Considering the relevance of the described safeguards, it is somewhat surprising that the Recommendation puts the responsibility for developing them on the service providers.

3-082 **Cooperation** The Recommendation encourages close cooperation between, on the one hand, the hosting services providers and, on the other hand, the judicial and administrative authorities of the Member States, the trusted flaggers (having the necessary expertise and determined on a clear and objective basis) and other hosting providers, in particular smaller ones which may have less capacity to tackle illegal content.[134]

3-083 **Stricter recommendation for terrorist content** Given the more detrimental nature of online terrorist content and building on the experience and practices acquired within the EU Internet Forum to counter terrorist content online, the Com-

[132] Commission Recommendation 2018/334 on measures to effectively tackle illegal content online, paras 9 to 13.

[133] Commission Recommendation 2018/334 on measures to effectively tackle illegal content online, paras 18 to 20.

[134] Commission Recommendation 2018/334 on measures to effectively tackle illegal content online, paras 22 to 28.

mission recommends more actions to the online platforms and the national authorities to detect and then remove such content.[135]

3. Sector-specific liability regimes

3-084 **Stricter specific regimes** The current policy debate is steadily shifting from intermediary liability to intermediary responsibility.[136] The former is understood as a negligence-based (ex post) approach while the latter emphasises the need for proactive measures (ex ante). The shift is visible in several initiatives of the EU institutions that steer in the direction of bestowing more responsibility on online platforms for regulating content, by requiring them to take certain proactive measures. The EU institutions have started implementing this approach by introducing amendments or new legislation in three different regulatory areas: audiovisual media services, copyright and terrorist content.

3-085 **Video-sharing platforms** The recently amended AVMS Directive imposes on video-sharing platforms the adoption of measures against some types of particularly harmful content prohibited by EU law (terrorism content, child pornography, and racism and xenophobia) as well as hate speech. Those measures should be proportionate to, on the one hand, the harm that may be caused and, on the other hand, the capacity of the platform to prevent such harm. They may be based on proactive measures or notice and takedown and should ensure a fair balance between the fundamental rights at stake.[137]

3-086 **Online content-sharing service providers using copyrighted content** The recently adopted Copyright DSM Directive strengthens the liability of providers of online content sharing services when they share copyrighted material. First, those specific types of online platforms do not benefit from the EU liability exemption of the Directive of electronic commerce when they give the public access to copyrighted material. Second, if they do not get a licence to share the material, online content-sharing service providers are liable of copyright violation unless they have: (i) made best efforts in obtaining an authorisation; (ii) made best efforts to ensure the unavailability of the copyrighted material for which rightholders have provided the necessary information; and (iii) acted expeditiously to disable access to copyrighted material upon notice from the rightholders.[138]

3-087 **Online terrorist content** In September 2018, the Commission tabled a proposal for a Regulation which aims to increase the obligation of all providers of hosting services to prevent the dissemination of terrorist content online.[139] This proposal, which is mainly turning into hard-law the recommendations of March 2018,[140] will reinforce the duty of care of online platforms and impose better detection and

[135] Commission Recommendation 2018/334 on measures to effectively tackle illegal content online, paras 29 to 40.

[136] Frosio "Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility" (2018) 26 *International Journal of Law and Information Technology* 1.

[137] AVMS Directive art.28b, analysed in para.4-140–4.145 of this book.

[138] Copyright DSM Directive art.17 analysed in Chapter VIII of this book.

[139] Proposal of the Commission of 12 September 2018 for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, COM(2018)640.

[140] Commission Recommendation 2018/334 on measures to effectively tackle illegal content online, paras 29 to 40.

quicker removal in case of terrorist content. However, this proposal has not yet been adopted by the European Parliament and the Council.

E. SELF- AND CO-REGULATION

3-088 **Effectiveness of self- and co-regulation in rapidly moving industries** Given the novelty and complexity of many issues and practices to be regulated and the important information asymmetry between the online platforms and the public authorities, self- or co-regulation may, in some circumstances, be more effective to achieve certain public policy goals.[141] The electronic commerce Directive encourages the trade, professional and consumer associations to draw-up, and then assess, codes of conduct contributing to a proper implementation of the rules of the Directive.[142] Online providers may also adopt codes of conduct that go further than the Directive. In that regard, the Commission has developed, by open consultation, principles for better self- and co-regulation that have been tested by pilot Community of Practice.[143] Those principles relate to the conception of the rules: they should be prepared openly and by as many as possible relevant actors; they should set clear targets and indicators and be designed in compliance with EU and national law. Principles also relate to the implementation of the rules: they should be monitored in a way that is sufficiently open and autonomous, improved in an iterative manner (learning by doing) and non-compliance should be subject to a graduated scale of sanctions.

3-089 **Use of codes of conduct to fight illegal and harmful online material** In the recent years, several codes of conduct have been adopted by the main online platforms to reduce the presence of illegal and harmful goods, content and material on the internet. In many cases, the platforms commit to more obligations than the ones imposed in EU law, often in order to prevent the adoption of stricter rules. The Commission is encouraging the development of those codes of conduct and is involved in the monitoring of their impact.

3-090 *Sale of counterfeit goods via the internet* In 2011, a *Memorandum of Understanding on the sale of counterfeit goods via the Internet* ("MoU") was signed between rights owners, internet platforms and associations. This MoU aimed to improve notice and takedown, and enhance proactive measures taken by rights owners and online intermediaries, increase cooperation and better fight against repeated infringements. A revised version of the MoU was signed in May 2016 to include key performance indictors in order to facilitate monitoring. The evaluation by the Commission shows that notice and takedown are useful and have been improved by the MoU but, because they are only applied ex-post, they need to be complemented by preventive and proactive measures.[144] Those measures require a close cooperation between intermediaries and rightholders. They can be supported by automated techniques, although such techniques tend to have many false positives (over-removal) which need to be corrected by human interventions.

[141] Self- and co-regulation is also encouraged for audiovisual media services (see AVMS Directive art.4a and paras 4-158 to 4-160 of this book) and, to a lesser extent, for electronic communications services (EECC art.24(2) analysed in para.2-43 of this book).

[142] Electronic Commerce Directive art.16.

[143] Those principles are available at: *https://ec.europa.eu/digital-single-market/en/best-practice-principles-better-self-and-co-regulation* [Accessed 16 September 2019].

[144] Commission Staff Working Document of 29 November 2017, Overview of the functioning of the Memorandum of Understanding on the sale of counterfeit goods via the internet, SWD(2017)430.

3-091 *Child sexual abuse and child sexual exploitation* In December 2011, a CEO "Coalition to Make the Internet a Better place for Kids" was launched with several objectives including the effective takedown of child abuse material.[145] The CEO Coalition worked to give increased transparency regarding takedown procedures and share best practices. It also worked with hotlines and law enforcement agencies to improve takedown times.[146] One year later in 2012, the *ICT Coalition for Children Online* was set up to deal with both illegal child sexual abuse material and inappropriate content.[147] Members include social networks, video platform providers, mobile operators and ISPs, content providers and others. The ICT Coalition meets twice yearly in a stakeholder forum to exchange information on new developments and members report every two years on their progress in implementing policies to improve the safety of children online. Then in February 2017, the *Alliance to Better Protect Minors Online*, a multi-stakeholder forum facilitated by the Commission, was set up in order to address emerging risks that minors face online, such as harmful content (e.g. violent or sexually exploitative content), harmful conduct (e.g. cyberbullying) and harmful contact (e.g. sexual extortion).[148] It is composed of actors from the entire value chain, including device manufacturers, telecoms, media and online services used by children. Its action plan includes the provision of accessible and robust tools that are easy to use and to provide feedback and notification as appropriate, the promotion of content classification when and where appropriate and the strengthening of the cooperation between the members of the Alliance and other parties (such as child safety organisations, governments, education services and law enforcement) to enhance best-practice sharing.[149]

3-092 *Terrorist content online* In December 2015, an "EU Internet Forum to counter terrorist content online" was established among EU Interior Ministers, high-level representatives of major internet companies (such as Facebook, Google, Microsoft and Twitter), Europol, the EU Counter Terrorism Co-ordinator and the European Parliament.[150] The Forum meets annually and has seen its membership expanded. One of its goals is to reduce accessibility to terrorist content online.

3-093 *Illegal hate speech online* In May 2016, a "Code of conduct on countering illegal hate speech online" was signed by some of the large online intermediaries (Facebook, Microsoft, Twitter, YouTube, Google+, Instagram and Snap Chat).[151] The Code aims at clear, accessible and effective notice-and-takedown procedures, removal of the majority of notices within one day and cooperation with trusted flaggers, in particular from civil society organisations and awareness campaigns. The

[145] See *https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids* [Accessed 16 September 2019].

[146] Summary report of the CEO Coalition working groups, available at *https://ec.europa.eu/digital-single-market/node/61973* [Accessed 16 September 2019].

[147] See *http://www.ictcoalition.eu* [Accessed 16 September 2019].

[148] See *https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online* [Accessed 16 September 2019].

[149] The common action is complemented by individual company commitments with a specific timeline to better protect minors online; see: *https://ec.europa.eu/digital-single-market/en/news/individual-company-statements-alliance-better-protect-minors-online* [Accessed 16 September 2019].

[150] Commission Press Release of 3 December 2015, IP/15/6243.

[151] See *http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300* [Accessed 16 September 2019].

implementation and impact of the Code is assessed every six months by the Commission.[152]

3-094 *Fake news and online disinformation* In October 2018, several online platforms, including Google, Facebook, Twitter and trade associations representing the advertising sector agreed to an "EU Code of Practice against disinformation".[153] The Code aims to (i) disrupt advertising revenue for accounts and websites misrepresenting information and provide advertisers with adequate safety tools and information about websites purveying disinformation; (ii) enable public disclosure of political advertising and make effort towards disclosing issue-based advertising; (iii) have a clear and publicly available policy on identity and online bots and take measures to close fake accounts; (iv) offer information and tools to help people make informed decisions, and facilitate access to diverse perspectives about topics of public interest, while giving prominence to reliable sources; and (v) provide privacy-compliant access to data to researchers to track and better understand the spread and impact of disinformation. The monitoring of the Code is part of the Action Plan against disinformation adopted by the Commission in December 2018 to build up capabilities and strengthen cooperation between Member States and EU institutions to proactively address the threats posed by disinformation.[154]

F. ENFORCEMENT

3-095 **Introduction** Contrary to the regulation of electronic communications or audiovisual media services, EU law does not foresee the establishment of specific national authorities for the regulation of information society services. The Directive on electronic commerce merely provides for the establishment of a national contact point to give to information society services providers' information on contractual rights and obligation as well as on the available complaint and redress mechanisms.[155] Therefore, enforcement of the rules mainly relies on the national Courts. However, as judicial actions may be complex, slow and expensive, EU law complements those with the internal complaint mechanisms and out-of-court dispute resolution mechanisms that may be quicker and less expensive. Moreover, as many online platforms are global, EU law encourages cooperation between national authorities.

1. National level

3-096 **Internal complaint-handling imposed on providers of online intermediation services** Providers of online intermediation services should (except if they are SMEs) put in place an internal complaint-handling system to enable business us-

[152] The fourth evaluation of February 2019 shows that online platforms are now assessing 89% of flagged content within 24 hours and 72% of the content deemed to be illegal hate speech is removed, compared to 40% and 28% respectively when the Code was first launched in 2016. However, online platforms still need to improve their feedback to users: Commission Press Release of 4 February 2019, IP/19/805.

[153] The Code is available at: *https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation* [Accessed 16 September 2019].

[154] Joint Communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 14 June 2019, Report on the implementation of the Action Plan Against Disinformation, JOIN(2019)12.

[155] Electronic Commerce Directive art.19(4).

ers to have access to immediate and effective redress, notwithstanding the possibility to resort to court proceedings.[156] These internal complaint-handling systems should be free of charge, based on the principles of transparency, equal treatment and be proportionate to the importance and complexity of the complaint. Platforms should also make available public information on the functioning and effectiveness of their internal complaint-handling system.

3-097 **Out-of-court dispute resolution** In addition to the obligations stemming from general consumer protection rules on alternative dispute resolution,[157] the electronic commerce Directive provides that national legislation should not hamper the use of out-of-court dispute settlement schemes between the providers and the users (hence going beyond the mere consumer) of information society services.[158]

3-098 *Mediation encouraged by providers' online intermediation services* The providers of online intermediation services are subject to more detailed and extensive rules, as they should identify two or more mediators with which the platform is willing to engage to try to reach an out-of-court settlement with a business user. Although the mediation process is voluntary, the Regulation specifies a number of criteria to be met by the designated mediators, while also giving the freedom to platforms and business users to jointly identify a mediator of their choice. Platforms should examine in good faith requests to engage in mediation. The Commission is expected to encourage the setting up of specialised mediation organisations with specialist knowledge of online intermediation services.[159]

3-099 **Collective action against providers of online intermediation services and search engines** Finally, to increase the effectiveness of judicial actions, the Regulation on fair treatment of business users of online platforms gives the right to organisations that represent business users or corporate website users and to public bodies set up by the Member States, to take action before the national courts in order to stop or prohibit any non-compliance with the Regulation. To alleviate any abuse, those organisations and public bodies should be designated by the Member States and mentioned in a Commission list published in the Official Journal.[160]

3-100 **Effective sanctions** As for any EU obligation, Member States should set up sanctions that are effective, proportionate and dissuasive in case of violation of the rules applicable to online platforms.[161]

2. European level

3-101 **EU cooperation between national authorities** Member States should cooperate with each other and with the Commission as well as provide mutual assistance

[156] Regulation on fair treatment of business users of online platforms art.11.

[157] Directive 2013/11 of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes (Directive on consumer ADR) OJ [2013] L 165/63, analysed in Chapter VII of this book.

[158] Electronic Commerce Directive art.17.

[159] Regulation on fair treatment of business users of online platforms, arts 12 to 13.

[160] Regulation on fair treatment of business users of online platforms art.14.

[161] Electronic Commerce Directive art.20; Regulation on fair treatment of business users of online platforms art.15.

for the implementation of the rules on information society services.[162] To facilitate this cooperation, the Commission has set up in 2005 an expert group on electronic commerce composed of the national contact point and chaired by the Commission.[163]

3-102 **EU Observatory for online platforms** In 2018, the Commission set up another expert group composed on independent experts to advise the Commission on the evolution of the online platform economy and possible EU actions in case of potential harmful practices.[164]

[162] Electronic Commerce Directive art.19.

[163] Commission Decision 2005/752 of 24 October 2005 establishing an expert group on electronic commerce [2005] OJ L282/20. The group is subject to the horizontal transparency rules applicable to the Commission expert groups: Commission Decision of 30 May 2016 establishing horizontal rules on the creation and operation of Commission expert groups, C(2016) 3301. The composition of the group, the agenda of the meeting and the documents discussed are available at: *https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=1636* [Accessed 16 September 2019].

[164] Commission Decision of 26 April 2018 on setting up the group of experts for the Observatory on the Online Platform Economy C(2018)2393. The group is also subject to the horizontal transparency rules applicable to the Commission expert groups: Commission Decision of 30 May 2016 establishing horizontal rules on the creation and operation of Commission expert groups, C(2016)3301. The composition of the group, the agenda of the meeting and the documents discussed are available at: *https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3607&NewSearch=1&NewSearch=1* [Accessed 16 September 2019].