The e-commerce Directive as the cornerstone of the Internal Market

DE STREEL, Alexandre; Husovec, Martin

Publication date:
2020

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

STUDY

Requested by the IMCO committee

European Parliament

The e-commerce Directive as the cornerstone of the Internal Market

Assessment and options for reform

Policy Department for Economic, Scientific and Quality of Life Policies
Directorate-General for Internal Policies
Authors: Alexandre de STREEL, Martin HUSOVEC
PE 648.797 - May 2020

EN

The e-commerce Directive as the cornerstone of the Internal Market

Assessment and options for reform

Abstract

The e-commerce Directive was adopted in 2000 and has played a key role in the development of online platforms in Europe. The study assesses the effects of the Directive as a cornerstone of the Digital Single Market. On that basis, it proposes some reforms for the future Digital Services Act.

This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies at the request of the committee on Internal Market and Consumer Protection (IMCO).

This document was requested by the European Parliament's committee on Internal Market and Consumer Protection

AUTHORS
Alexandre de STREEL, University of Namur and Centre on Regulation in Europe (CERRE)
Martin HUSOVEC, London School of Economics and Political Science (LSE)

ADMINISTRATORS RESPONSIBLE
Mariusz MACIEJEWSKI
Christina RATCLIFF

EDITORIAL ASSISTANT
Irene VERNACOTOLA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for email alert updates, please write to:
Policy Department for Economic, Scientific and Quality of Life Policies
European Parliament
L-2929 - Luxembourg
Email: Poldep-Economy-Science@ep.europa.eu

Manuscript completed: May 2020
Date of publication: May 2020

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

CONTENTS

LIST OF ABBREVIATIONS

ADR	Alternative Dispute Resolution
AI	Artificial Intelligence
AVMSD	AudioVisusal Media Service Directive
B2B	Business-to-Business
B2C	Business-to-Consumer
CEN	Comité Européen de Normalisation – European Committee for Standardisation
CENELEC	Comité Européen de Normalisation en Electronique et en Electrotechnique European Committee for Electrotechnical Standardisation
CPC	Consumer Protection Cooperation
DSA	Digital Services Act
DSM	Digital Single Market
DSMD	Copyright in Digital Single Market Directive
ECB	European Central Bank
ECD	Electronic Commerce Directive
EECC	European Electronic Communications Code
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
IMI	Internal Market Information System
IP	Intellectual Property
ISS	Information Society Service
JRC	Joint Research Centre
NGO	Non-Governmental Organisation

NIS	Network and Information Security Directive
ODR	Online Dispute Resolution
OECD	Organisation for Economic Co-operation and Development
P2B	Platfom-to-Business Regulation
SME	Small and medium-sized enterprises
TFEU	Treaty on the Functioning of the European Union
UCPD	Unfair Commercial Practices Directive
UK	United Kingdom
US	United States

LIST OF TABLES

EXECUTIVE SUMMARY

Background

The scope and the pillars of the e-commerce Directive and the evolution of the EU legal framework regarding e-commerce.

The e-commerce Directive has a **very broad scope** as it covers any service provided at a distance by electronic means at the individual request of a recipient, so most of the digital services we have become accustomed to use. The Directive was adopted in 2000 at a time when online platforms were in their infancy and many current technologies and applications did not exist yet.

The Directive is composed **of four main pillars which aim to stimulate the development of online platforms and e-commerce in Europe while protecting the users** of those platforms: (i) the country of origin, (ii) the harmonisation of some user protection rules, in particular transparency, (iii) exemption of liability for illegal online content in favour of some platforms and under some conditions and (iv) promotion of smart regulatory techniques and enforcement.

Since the adoption of the Directive in 2000, the **Court of Justice of the EU has clarified the scope** of the Directive which applies to some collaborative economy platforms, has **affirmed the country of origin** principle and has **tried to delineate the frontiers of the liability exemption**. However for liability, some issues still lead to divergent interpretation across the Member States.

Since the adoption of the Directive, **many new rules and enforcement tools and institutions** relating to the providers of Information Society Services, what is often now referred as online platforms, have been adopted at the EU level,

- Some of those rules **target specific categories of Information Society Services** and aim to increase transparency and security requirements for intermediation and search services, and to introduce measures to address specific concerns such as illegal and harmful content, online disinformation and advertising for video sharing platforms or the payment of copyright by online content sharing platforms. In addition, several codes of practices have been adopted by the main online platforms to better tackle illegal and harmful content. With the adaption of those new rules, a **more complex picture of online platforms regulation is emerging**. The ECD is the general and horizontal regime. This baseline is then complemented by stricter rules applicable either to specific types or sizes of platforms or to specific types of online illegal content or products. Those stricter rules reflect the application of a risk-based approach and proportionality principle;
- **Other rules are more general** and apply to providers of all types of services, information society or others, in order to improve the fundamental freedoms of movement in the EU, consumer protection, data protection. They also aim to improve cooperation between Member States or alternative regulatory mechanisms such self - and co-regulation or out-of-court dispute resolution.

Member States are also adopting some **national laws**, in particular to reinforce the measures that online platforms should take to tackle illegal content online. However, those national laws carry serious risks of **undermining the completion of the Digital Single Market**.

The Evaluation of the e-commerce and its impact on the Internal Market.

The European Commission did **three main waves of evaluation** of the e-commerce Directive and more generally of the EU rules and policies on digital platforms.

In the first evaluation which took place in **2003** when the Directive was about to be transposed by the Member States, the Commission observed **positive trends**, in particular a reduction in Court proceedings on the liability of digital platforms and overall satisfaction of the country of origin principle.

In the second evaluation which took place in **2011 - 2012**, the Commission found that the **principles and the rules of the ECD were sound**, but that some improvements were needed, in particular regarding the Notice-and-Takedown systems.

In the third evaluation which took place in **2016 - 2017**, the Commission found again that the principles and the rules of the ECD were sound. However, the Commission observed the **increasing importance of online platforms and the new risks of Digital Single Market fragmentation.** This led to three-pronged strategy: (i) adapt sectoral hard-law when there is a specific problem; (ii) give more guidance on the interpretation of the less clear provisions of the e-commerce Directive, in particular regarding the Notice-and-Takedown and the reliance on voluntary preventive measures; and (iii) encourage coordinated EU-wide co and self-regulation for the illegal materials which are particularly harmful.

Academic studies identified that the underlying **notice and takedown framework generally is exposed to the following trends**: the quality of notifications sent to the providers is often very low (at least in some areas); there is a diverging quality of such notifications among different notifiers; the notifications are increasingly out-sourced to professional companies; increasingly, the notifications are sent by algorithms, and not humans; providers tend to over-remove content to avoid liability and save resources; they equally employ technology to evaluate the notifications; the affected users who posted content often do not take action.

The **e-commerce Directive is one of the cornerstones of the Digital Single Market** which, with the increasing digitisation of the economy and the society, should now underpin the whole Internal Market project.

Our assessment of the e-commerce Directive and our recommendations for the forthcoming Digital Services Act.

The definition of the **Information Society Service**, which determines the scope of the ECD, proves to be **robust over time** and applicable to new business models. The concerns raised by some that the no prior authorisation rule applicable to ISS severely limits the competence of the Member States to regulate the underlying services intermediated by **collaborative economy** platforms, such as transport or hosting, have proven to be unfounded.

The **Internal Market Clause is one of the greatest successes** of the e-commerce Directive. To be accepted and effective, such clause requires trust between Member States that the regulation in the country of origin is sufficiently protective and effectively enforced. In turn, this requires the EU harmonisation of the main protection rules and effective cooperation between national authorities. Fortunately since the adoption of the ECD, both have increased. Thus, in any review of the ECD, **the country of origin should absolutely be maintained while the cooperation between Member States could be strengthened** and better organised in order to make the procedure more efficient and rapid, in particular between the country of origin and the country of destination where the provider is offering its services.

Moreover, the ECD and its Internal Market Clause, could also be **extended to cover the online platforms which are not established in the EU** but provide their services to EU customers, for instance by requiring the designation of a representative in the EU.

The criticism of the Directive's **liability rules** can be grouped as follows: (1) the Directive lacks sufficient safeguards to prevent violations of fundamental rights, in particular freedom of expression; (2) the Directive does not envisage that notifications may be sent by robots and fails to incentivise the quality of sent and reviewed notifications; (3) the Directive does not prevent fragmentation due to diverging application of the passivity criterion by the national courts; (4) the Directive fails to cover hyperlinking and search engines and other new services; (5) the Directive only serves as a limit and not as a comprehensive tool of removal of illegal content. Each of these points demands a response when updating the ECD.

It is proposed that the new law: (1) prescribes strong, swift and scalable **remedies against over-removal of legitimate content,** including through an external ADR (that would be financed by higher fees paid by providers which erroneously take down the content and lower fees by users who complain without success) to incentivise better internal quality review; (2) sets concrete **incentives for high-quality notification and review** process by means of elaborate rules developed through technical standardisation in different areas; (3) clarifies the **passivity criterion by linking it to editorial choices** and thereby avoiding discouragement of voluntary preventive measures; (4) includes a set of **new safe harbours**, at least for hyperlinks, search engines and domain name authorities; and (5) creates an EU-wide legal basis for **targeted measures** (preventive or corrective) responding to the risks posed by the hosting providers provided that the evidence suggests a failure the notice and takedown process and that they remain compliant with the no monitoring obligation and fundamental rights.

Since the adoption of the ECD in 2000, many EU legislations and enforcement tools and institutions relating to the provision of Information Society Services have been adopted (some are more general and covering all services provided in the EU Internal Market while others are more specific and cover only specific categories of Information Society Service). It is essential that **the puzzle rules applicable to online platforms and their enforcement mechanisms are coherent and effective.** ECD should be made consistent with those new general rules, in particular by streamlining transparency and information requirements. Also the regulation of the different types of Information Society could be more coherent, in particular by improving the baseline liability regime of online platforms (as explained above) and by strengthening the regulation of online advertising. For those two issues, the new rules imposed by the **Audio-visual Media Services Directive (AVMSD)** on the video-sharing platforms are a **good starting point**.

Smart regulatory techniques such as **self- and co-regulation should continue to be encouraged** given the rapid and uncertain market evolution as well as the exponential increase of online content. However, to respect our EU values, in particular our human rights and rule of law, **better safeguards need to be set up**. In particular, Codes of conduct should be accepted by the main stakeholders representing all the interested parties and values and that their implementation should be regularly monitored in a transparent and independent manner.

The revision of the ECD which is the horizontal and applicable to all the providers of Information Society Services in Europe could be accompanied by **two complementary reforms** within the Digital Services Act to take technology and market developments into account.

- The first complementary reform could **increase the incentives for data sharing and mobility.** Given that sectors differ widely, it would be advisable to use experimental regulatory techniques (such as regulatory sandbox), legislation with sunset clauses and time-limited incentive-based schemes. Moreover, a distinction between personal and non-personal data should be avoided. Any data sharing should actively engage with data protection framework, even if the exposure to its might be only marginal in practice;
- The second complementary reform could consist in the adoption of **stricter rules for the online platforms raising systemic risks** to the European economy and society. Such asymmetric rules could deal with market power issues that cannot be effectively dealt with by pure ex post competition law and ensure that the markets remain fair and contestable. They could also deal with the diffusion of online illegal and harmful content. Those asymmetric rules **could be enforced by an EU regulator** to ensure effectiveness and internalise the cross-countries externalities but **in close partnership with the national regulatory authorities** to meet the principle of subsidiarity. In that regard, the enforcement of financial regulation on the systemic banks by Single Supervisory Mechanism within the ECB is an interesting starting point. At the very minimum, the coordination between national regulatory authorities and the division of work between them should be improved and ensure an effective law enforcement.

1. SCOPE AND OBJECTIVES OF THIS STUDY[1]

The study reviews the key role played by the e-commerce Directive (further referred to as "ECD") in building the Digital Single Market over the last 20 years.[2] The aim of this report is to provide indications for the IMCO Committee of the European Parliament whether a reform of the Directive is necessary and to provide specific recommendations on the key elements of such a reform and the possible scope and content of the future Digital Services Act announced by the Commission in its Digital Strategy Communication of February 2020.[3]

This report is part of a broader project containing seven other independent in-depth analyses covering the following issues,

- (i) the **legal framework for e-commerce** in the Internal Market: State of play, remaining obstacles to the free movement of digital services and ways to improve the current situation;
- (ii) how to fully reap all the benefits of the Internal Market for e-commerce? **New economic opportunities** and challenges for digital services 20 years after the adoption of the e-commerce Directive;
- (iii) the functioning of the Internal Market for digital services: **Responsibility and duty of care** of providers of digital services. Challenges and opportunities;
- (iv) new developments and **innovations brought by Artificial Intelligence** applied to e-commerce: challenges to the functioning of the Internal Market;
- (v) **enforcement** and cooperation between Member States;
- (vi) possible **new aspects** and challenges in the field of **consumer protection**;
- and (viii) new **developments of digital services**.

This report is composed of four Sections: after this introduction, Section 2 explains the objectives and the pillars of the e-commerce Directive and reviews the main legislative and judicial development that took place at the EU level since the adoption of the ECD in 2000. Section 3 reviews the evaluations that have been done on the ECD as well as the effects on the ECD on the Internal Market. Section 4 gives our own assessment of the ECD and, on that basis, proposes some recommendations to improve the ECD.

[1] The authors want to thank Michèle Ledger and Yves Poullet for their very helpful comments and suggestions.

[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 (Directive on electronic commerce), OJ [2000] L 178/1.

[3] Communication from the Commission of 19 February 2020, Shaping Europe's digital future, COM(2020) 67, p.12.

2. E-COMMERCE DIRECTIVE AND THE EVOLUTION OF THE LEGAL FRAMEWORK

KEY FINDINGS

The e-commerce Directive has a **very broad scope** as it covers any service provided at a distance by electronic means at the individual request of a recipient, so most of the digital services we have become accustomed to use. The Directive was adopted in 2000 at a time when online platforms were in their infancy and many current technologies and applications did not exist yet.

The Directive is composed of **four main pillars which aim to stimulate the development of online platforms and e-commerce in Europe while protecting the users** of those platforms: (i) the country of origin, (ii) the harmonisation of some user protection rules, in particular transparency, (iii) exemption of liability for illegal online content in favour of some platforms and under some conditions and (iv) promotion of smart regulatory techniques and enforcement.

Since the adoption of the Directive in 2000, **the Court of Justice of the EU has clarified the scope** of the Directive which applies to some collaborative economy platforms, has **affirmed the country of origin** principle and has **tried to delineate the frontiers of the liability exemption**. However for liability, some issues still lead to divergent interpretation across the Member States.

Since the adoption of the Directive, **many new rules and enforcement tools and institutions** relating to the providers of Information Society Services, what is often now referred as online platforms, have been adopted at the EU level.

- Some of those rules **target specific categories of Information Society Service** and aim to increase transparency and security requirements for intermediation and search services, and to introduce measures to address specific concerns such as illegal and harmful content, online disinformation and advertising for video sharing platforms or the payment of copyright by online content sharing platforms. In addition, several Codes of practices have been adopted by the main online platforms to better tackle illegal and harmful content. With the adaption of those new rules, a **more complex picture of online platforms regulation is emerging**. The ECD is the general and horizontal regime. This baseline is then complemented by stricter rules applicable either to specific types or sizes of platforms or to specific types of online illegal content or products. Those stricter rules reflect the application of a risk-based approach and proportionality principle.

- **Other rules are more general** and apply to providers of all types of services, information society or others, in order to improve the fundamental freedoms of movement in the EU, consumer protection, data protection. They also aim to improve cooperation between Member States or alternative regulatory mechanisms such self- and co-regulation or out-of-court dispute resolution.

Member States are also adopting some **national laws**, in particular to reinforce the measures that online platforms should take to tackle illegal content online. However, those national laws carry serious risks of **undermining the completion of the Digital Single Market**.

2.1. The e-commerce Directive

2.1.1. Objectives of the ECD

The e-commerce Directive was adopted in June 2000, and its transposition deadline expired in January 2002. The development of information society services within the area without internal frontiers was considered vital to eliminating the barriers which divide the European peoples.[4] The Directive was particularly meant to stimulate cross-border trade by removing legal obstacles to the exercise of the **freedom of establishment and the freedom to provide services** stemming from divergences in legislation, legal uncertainty as to which national rules apply and the extent to which Member States may control services originating from another Member State.[5] It uses the minimum harmonisation approach.[6]

The Directive was adopted as a complement to other EU legislative initiatives addressing the development of e-commerce and in particular issues linked to data protection,[7] consumer protection,[8] electronic signatures,[9] and copyright.[10] These initiatives aimed to increase the trust of users in the online environment, coordinate rules between the Member States while also fostering the development of the information society by defining minimum rules on the roles and responsibilities of certain players. While not addressing human rights directly, the Directive recalled the importance of values like freedom of expression, privacy, confidentiality of information or anonymity.[11]

2.1.2. Scope and pillars of the ECD

The ECD applies to the provision of Information Society Services (further referred to as "ISS") and is based on four main pillars: (i) freedom to provide ISS in each Member State and across the whole Internal Market, (ii) protection of users, (iii) harmonised EU exemptions of national liability regimes for some providers of ISS and (iv) mechanisms to ensure effective enforcement of the rules.

(i) Scope of the Directive: The Information Society Service

The e-commerce Directive approximates national provisions related to the provision of ISS[12] which are defined by reference of the *Transparency Directive* as '**any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient**'.[13]

---

4 ECD, Recital 1; Most of the Commission documents related to the preparation and the adoption of the ECD in 2000 and the evolution of the EU legal framework since then are available at: https://ec.europa.eu/digital-single-market/en/news/archive-e-commerce-directive-what-happened-and-its-adoption.

5 ECD, recital 5. Also Explanatory Memorandum of the Commission proposal for a Directive on certain legal aspects of electronic commerce in the internal market, COM(1998) 586, pp. 6-10.

6 ECD, Art.1 and recital 10.

7 Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Directive has now been replaced by Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation), OJ [2016] L 199/1.

8 In particular, Directive 97/7 of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ [1997] L 144/19. This Directive has now been replaced by Directive 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, OJ [2011] L 304/64, as amended by Directive 2019/2161. Other EU consumer protection law applicable at the times of the adoption of the ECD are mentioned at recital 11.

9 Directive 1999/93 of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. This Directive has now been replaced by Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, OJ [2014] L 257/73.

10 Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ [2001] L 167/10. This Directive is now complemented by 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, OJ [2019] L 130/92.

11 ECD, Recitals 9, 14 and 15.

12 ECD, Art.1(1) and 2(a).

13 Directive 98/34 of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, OJ [1998] L 204/37 as amended by Directive

However, the ECD does not apply to some areas and activities, the main ones being 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.[14]

(ii) Freedom to provide Information Society Services in and across Member States

The first pillar of the ECD aims to facilitate the provision of Information Society Services with two main rules. First, the Member State **cannot impose prior authorisation** or any requirement having equivalent effect to provide an ISS, without prejudice to authorisation schemes which are not specifically and exclusively targeted at ISS.[15]

Second, for the rules covered by the "coordinated field",[16] the provider of ISS **can offer the service in all the other Member States by merely complying with the rules of the country of establishment** (country of origin) and should not comply with additional rules in the country where the ISS is offered (country of destination). Thus, the ISS provider cannot face any restriction from another Member State. The ECD provides for two categories of **exceptions** to this Internal Market rule,

- The first category is **general** and applies to eight fields mentioned in the Annex of the ECD.[17] In practice, the main areas of relevance are matters covered by intellectual property rights, contractual obligations concerning consumer contacts and the freedom of the parties to choose the law applicable to their contracts;
- The second category is a **case-by-case** exception and may be used at the request of the Member State of destination under strict material (in particular, proportionate measures to protect public interest) and procedural conditions (in particular, notification to the Commission and other Member States).[18]

(iii) Protection of Users

The second pillar of the ECD aims to protect users in general (i.e. consumers, business users, public authorities) by harmonising certain obligations, mainly related to transparency, which are imposed on ISS providers.

First, ISS providers must make available **their identity**, name, geographic address, and details enabling rapid contact, and relevant registration information (in trade or similar registers), VAT number where relevant. If the activity is subject to a specific authorisation scheme, elements to identify the competent supervisory authority should also be made available.[19]

Second, **commercial communications** 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

98/48, Art. 1(2). This Directive is now replaced by the 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, OJ [2015] L 241/1, Art.1(b).

14 ECD, Art.1(5).

15 ECD, Art.4.

16 A special feature of the ECD 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 ISS, such as requirements concerning qualifications, authorisation or notification, the pursuit of the activity of an ISS, 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. 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: ECD, Art. 2(h).

17 ECD, Art.3(3) and Annex.

18 ECD, Art.3(4). For more details, see de Streel, Kuczerawy and Ledger (2019: paras 3-018 to 3-025).

19 ECD, Art.5.

exercising a regulated profession must clearly identify: the commercial communication itself; and the natural or legal person on 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.[20]

Third, the ECD makes sure that **contracts can be concluded electronically**. 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.[21] The ECD 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. Further, some minimum 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.[22]

(iv) Liability rules

The third pillar of the ECD aims to harmonise liability risks associated with the operation of the most common types of services that existed at the time of adoption of the Directive. Amid local developments in some countries which tried to hold intermediaries strictly liable for their user's content, the ECD opted for a model which **shares the burden of identification and removal of content among several stakeholders**.

Safe harbours included in Section 4 of the e-commerce Directive were inspired by the U.S. *Digital Millennium Copyright Act*; but they also feature some important differences.[23] Unlike the U.S. counterpart, the ECD only covers **three types of services: hosting, caching and mere conduit**, thus excluding information locations tools, such as search engines.[24] Linking and search engines can, however, be subject to national provisions.[25] In fact, Spain and Portugal have opted for the model of Art. 14 both for search engines and hyperlinks, whereas Austria have opted for the model of Art. 12 for search engines and of Art. 14 for hyperlinks.[26] All three safe harbours only cover situations when an ISS consisting of a particular technical activity (transmission/access; caching; storage) deals with 'information provided by a recipient of the service'.

Hence, they do not apply to the service provider's own editorial content.[27] Generally, entire Section 4 applies to technical activities undertaken within services provided by intermediaries; one service might consist of several activities (e.g. storage and access to information).

The three safe harbours create a **basic framework harmonising the point up until which the service providers cannot be held liable for third party information**.

[20] ECD, Art.6.
[21] ECD, Art.9.
[22] ECD, Art.10.
[23] Peguera (2009a).
[24] Peguera (2009b).
[25] ECD, Art.21(2) which was used by some of the Member States.
[26] Report of the Commission of 21 November 2003 on the application of Directive on electronic commerce, COM(2003) 702.
[27] Case C-291/13 *Papasavvas* EU:C:2014:2209.

The ECD did not harmonise the moment when liability for third party information is established, however. This part was left to the national law.

The design is partly due to the fact that the development of digital single market was at an early stage but also because the safe harbours limit all kinds of liability, including civil, administrative and criminal, as well as diverse areas of law. Creating a one set of uniform rules establishing liability in all these areas was not feasible. At the same time, undeniably, in some areas, national courts sometimes assume that once the safe harbours are lost, providers become ipso facto liable.

Each safe harbour comes with a carve-out for possibility for a court or administrative authority, in accordance with Member States legal systems, **of requiring the service provider to terminate or prevent an infringement**.[28] The legal basis for these correcting or preventive measures has to be found in the national law. However, in some areas, such as intellectual property law, EU law provides for such legal basis EU-wide.[29] These carve-outs allow duties of corrective or preventive character to be imposed, irrespective of the application of the safe harbours. Hence even if a hosting safe harbour applies, corrective and preventive measures can be imposed by the Member States. Both types of measures are however **limited in their scope and reach by the prohibition of general monitoring** included in the ECD.

The **general monitoring prohibition** in Art. 15 applies only when one of the safe harbours does too. It is addressed equally to the legislators and courts. According to it, 'Member States shall not impose a general obligation on providers (…) to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity'. The prohibition completes the three safe harbours, in the context of acceptable corrective and preventive duties under the carve-outs,[30] but also gives an interpretative guidance concerning conditions in Art. 12-14 ECD.

The ECD **left open a number of issues** for a potential review,

- First, the potential extension of safe harbours to other services in light of technological developments, in particular for hyperlinks and search engines which were consciously omitted;[31]
- Second, the introduction of 'notice and take down' procedures, which would govern the exchange of notifications;[32]
- Third, the attribution of liability following the taking down of content.[33]

The ECD thus left room to the Member States to experiment on these areas and other issues, such as notification obligations regarding illegal content,[34] administrative and judicial preventive ad hoc preventive measures,[35] or details concerning the notice and takedown process.

[28] ECD, Art. 12(3), Art.13(2), Art.14(3).
[29] IP Enforcement Directive, Art.11, third sentence.
[30] *See* Husovec (2017b).
[31] ECD, Art. 21(2).
[32] Ibid.
[33] It is not entirely clear if this was meant to concern only providers, or also other parties in the process, in particular the notifiers.
[34] ECD, Art. 15(2).
[35] ECD, Art. 12(3); Art. 13(2); Art. 14(3); Art.18.

(v) Mechanisms for effective enforcement

The fourth pillar of the ECD aims to ensure its effective enforcement which is key because, as often in the EU, the rules are decided at the European level but are enforced at the national level. First, the ECD sets some **safeguards about the national enforcement mechanisms** to ensure their effectiveness.

The sanctions in case of violation of the ECD rules should be effective, proportionate and dissuasive.[36] Further, the available national court actions should be effective allowing for the rapid adoption of corrective measures, including interim measures.[37]

Second, the ECD encourages **cooperation and mutual assistance between Member States and with the Commission** for the implementation of the rules on ISS, in particular through the establishment of national contact points.[38] Given the application of the 'country of origin' principle, it is key to have an effective cooperation between the Member State where the ISS provider is established and regulated and the Member State of destination where the ISS is offered. The ECD also provide for the procedural conditions if the Member State of destination wants derogate to the country of origin principle and regulate the provider of ISS.[39]

Third, the ECD encourages the reliance on **alternative enforcement modes** such as conclusion of codes of conduct at the EU level[40] or out-of-court dispute settlement schemes.[41]

2.2. Developments in EU case law

Since the adoption of the e-commerce Directive in 2000, the Court of Justice of the European Union, answering the preliminary ruling questions raised by national judges, clarified the content of several key concepts of the Directive. Those clarifications relate in particular to the definition of Information Society Service, the scope and the effects of the Internal Market Clause, the scope of the liability exemption and the scope the general monitoring prohibition.

2.2.1. Scope of the Directive: the definition of the Information Society Service

As the e-commerce Directive applies to the Information Society Service, the precise meaning of ISS and the legal qualification of a specific service provision are key to determine the scope of the ECD. While an ISS should normally be **provided for remuneration**,[42] the Court of Justice decided in *Papasavvas* and *Mc Fadden* that the ISS does not have to be paid by the recipient of the service (and can be free for her) but the service can be paid with income generated by advertisements.[43]

Moreover, the ISS qualification issue is particularly important in the context of the **collaborative economy** to determine whether the platforms providing collaborative services could be considered as providers of ISS and, thereby benefit from the rights of the ECD (in particular, the no prior authorisation rule and the Internal Market Clause).

[36] ECD, Art.20.
[37] ECD, Art.18.
[38] ECD, Art.19.
[39] ECD, Art. 3(4b).
[40] ECD, Art. 16.
[41] ECD, Art. 17.
[42] Transparency Directive 2015/1535, Art. 1(1b) which applies the case-law on the notion of service under Art. 56 TFEU.
[43] Case C-291/13 *Papasavvas* EU:C:2014:2209, paras.29-30 ; Case C-484/14 *Tobias McFadden v. Sony Music* EU:C:2016:689, paras.42-43.

In *Uber Spain* and *Uber France*, the Court of Justice decided that intermediation service offered by Uber formed an integral part of an overall service whose main component is a transport service and, accordingly, must be classified as a transport service and not as an ISS.[44]

Applying the rule '*l'accessoire suit le principal*', the Court of Justice determined what was the main service offered and then qualified all accessories according to this main service.[45]

In this case, the Court determined that online intermediation was merely accessory because Uber provided drivers with an app which if it was not used, the transport service would not have taken place and Uber exerted a decisive influence over the conditions under which the transport service was provided by setting the fare, controlling the quality of the vehicles or setting minimum safety standards.[46]

Applying the same approach and criteria to *Airbnb Ireland*, which has another business model than Uber, the Court of Justice decided that Airbnb was providing an ISS because it does not exercise decisive influence over the conditions under which the hosting services are provided.[47] In this case, the Court of Justice determined that online intermediation was the main service provided by Airbnb that can be separated from the hosting transaction itself and that cannot be regarded as forming an integral part of an overall service, the main component of which is the provision of accommodation.[48]

2.2.2. Internal Market rules

In *eDate Advertising*, the Court of Justice decided that, according to the **Internal Market Clause** of the ECD, Member States must ensure that, in relation to the 'coordinated field' and subject to the derogations authorised, the provider of an ISS is not made subject to stricter requirements than those provided for by the substantive law applicable in the Member State in which that service provider is established.[49] The Court also noted that the Internal Market Clause is not a specific conflict-of-laws rule.

Furthermore, in *Cornelius de Visser*, the Court of Justice decided that the Internal Market Clause does not apply to a situation where the place of establishment of the ISS provider is unknown since application of the clause is subject to identification of the Member State in whose territory the service provider in question is actually established.[50]

With regard to the scope of the **'coordinated field'** to which the internal clause applies, the Court of Justice decided in *Ker-Optika* that the coordinated field covers the online selling of contact lenses but does not cover the physical supply of contact lenses as the former is online while the latter is not.[51] Furthermore in *Vandenborght* the Court of Justice decided that the coordinated field covers a national law imposing a general and absolute prohibition of any advertising relating to the provision of dental care services, inasmuch as it prohibits any form of electronic commercial communications, including by means of a website created by a dentist.[52]

---

[44] Case C-434/15 *Asociación Profesional Élite Taxi v Uber Systems Spain* EU:C:2017:981, para.40 ; Case C-320/16, *Uber France* EU:C:2018:221, para. 22.

[45] The Court of Justice follows the approach proposed by the Commission according to which, 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: Communication from the Commission of 2 June 2016, A European agenda for the collaborative economy, COM(2016)356, p.6.

[46] Case C-434/15 *Asociación Profesional Élite Taxi v Uber Systems Spain*, para.39; Case C-320/16, *Uber France*, para.21.

[47] Case C-390/18, *Airbnb Ireland* EU:C:2019:1112, para.69.

[48] Case C-390/18, *Airbnb Ireland*, paras. 53 and 57.

[49] Joined Cases C-509/09 and C-161/10 *eDate Advertising* and *Martinez v. MGN* EU:C:2011:685.

[50] Case C-292/10 *Cornelius de Visser* EU:C:2012:142.

[51] Case C-108/09 *Ker-Optika* EU:C:2010:725.

[52] Case C-339/15 *Vanderborght* EU:C:2017:335, para.50. Also, Case C-949/18 *A v. Daniel B et al.*, Opinion of AG Saugmandsgaard Oe, EU:C:2020:134.

Finally with regard to the **derogation clause**, the Court of Justice decided in *Airbnb Ireland* that if a Member State takes measures that derogate from the principle of the freedom to provide ISS without complying with the procedural conditions of the ECD (in particular, the notification to the Commission and the other Member States), those measures cannot be applicable against such provider of an ISS.[53]

2.2.3. Liability rules

An absolute majority of cases dealing with the ECD's rules on intermediary liability dealt with intellectual property law. Starting in 2010, the case-law clarified that a number of **services can qualify for one of the safe harbours**, such as a social network,[54] an online marketplace,[55] keyword advertising service,[56] Internet access providers[57] or Wi-Fi operators.[58]

The Court of Justice clarified that although ECD does not harmonise the procedures for acquiring knowledge, it requires hosting providers to behave as diligent economic operators.[59] The **actual knowledge** envisaged in Art. 14 ECD requires knowledge about illegality of information, and not just its existence.[60] Furthermore, according to the Court of Justice, the notifications have to be 'sufficiently precise or adequately substantiated' to trigger actual knowledge.[61] General awareness would not be sufficient to lead to a loss of Art. 14 ECD.[62] The criteria for knowledge are therefore very open, and so far are understood to permit a broad range of solutions on the national level. The same would apply for potential EU-legislated upgrades.

By far, the biggest focus of the case-law was on two issues: (i) scope of the hosting safe harbours under Art. 14 ECD, and (ii) possible preventive duties which are not in violation of Art. 15 ECD.

Scope of the hosting safe harbour. In *Google France*, the Court of Justice postulated that all the safe harbours are limited by a general **requirement of passivity**, also referred to as a 'neutrality condition'.[63] The condition of passivity is tested by asking whether '[an] operator has not played an active role allowing it to have knowledge or control of the data stored'.[64] An instance of such a role is when the operator of an online marketplace 'provides assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them'.[65] At the same time, however, 'the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability'.[66] An active intervention would disqualify the provider for Art. 14 with respect to that particular piece of third-party information.

The passivity criterion became the most controversial and led to the diverging outcomes on the national level because it allowed national courts to easily side-step the ECD.[67]

---

53 Case C-390/18, *Airbnb Ireland*, para. 100. Thus the Court of Justice decided to impose the same sanction (unenforceability against individuals) for failure to notify in the context of the ECD and in the context of the Transparency Directive 2015/1535.
54 Case C-360/10 *SABAM v. Netlog* EU:C:2012:85; Case C-18/18, *Glawischnig-Piesczek v. Facebook Ireland* EU:C:2019:821.
55 Case C-324/09 *L'Oreal and* Others v. eBay and Others EU:C:2011:474.
56 Cases C-236/08 to C-238/08 *Google France and Google v. Vuitton* EU:C:2010:159.
57 Case C-70/10 *Scarlet v. Sabam* EU:C:2011:771; Case C-314/12 *UPC Telekabel Wien* EU:C:2014; Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten* EU:C:2009:107; Case C-461/10 *Bonnier Audio and Others* EU:C:2012:219.
58 Case C-484/14 *Tobias McFadden v. Sony Music* EU:C:2016:689.
59 See Case C-324/09 *L'Oreal and Others*.
60 Cases C-236/08 to C-238/08 *Google France and Google*, para 109 ("of the unlawful nature of those data or of activities of that recipient").
61 Case C-324/09 *L'Oréal*, para 122.
62 Husovec (2017a) p. 53 and the sources there.
63 Cases C-236/08 to C-238/08 *Google France and Google*, para 114, 120
64 Case C-324/09 *L'Oreal and Others* para. 113; Cases C-236/08 to C-238/08 *Google France and Google*, paras. 114 and 120.
65 Case C-324/09 *L'Oreal and Others*, para. 116; this language then re-appears in Art. 2(6) DSMD.
66 Ibid., para. 115.
67 See Nordermann (2018); Sartor (2017); Van Eecke (2011).

Specific preventive duties. The ECD does not prescribe preventive duties. However, it foresees them by permitting some of such measures. It refers to them as 'specific monitoring' or 'duties of care'.[68] It imposes two explicit limits: (i) conditions of carve-outs in each of the safe harbours; and (ii) prohibition of the general monitoring obligation. As a result, the national courts or legislators can impose specific preventive duties, which comply with these two statutory criteria and the EU Charter on Fundamental Rights as an overall limit.

The case-law dealing with the question of what type of preventive duties are permissible is in flux. The majority of cases is again driven by intellectual property disputes, given that EU law provides a legal basis in this area. On one hand, the Court of Justice to date rejected abstract non-targeted filtering which was requested against a social network and an Internet access provider.[69] On the other hand, it accepted *judicially imposed*,

- measures against repeated infringers by a trading platform;[70]
- blocking of a specific website by an Internet access provider;[71]
- password-locking by an open Wi-Fi operator;[72] and
- reliance on automated measures tackling general re-appearance of identical and in essence unchanged content to one which a court previously declared to be defamatory, as long as they do not require independent human assessment for precision.[73]

The case-law concerning specific duties is in development and greatly influences also legislative measures that complement the ECD framework. As mentioned later, the preventive duties anchored in the new Copyright Directive have to be equally specific,[74] and preventive duties in the revised Audio-visual Media Services Directive cannot 'lead to any ex-ante control measures or upload-filtering of content which do not comply with Art. 15 ECD'.[75] It will be the task of the upcoming case-law to clarify what exact measures are acceptable, and under what circumstances. The Court of Justice is playing an important role as an engine of harmonization in this context.

The last related area concerns data protection. ECD has a complicated relationship with the data protection framework, including GDPR.[76]

The Court of Justice is increasingly involving hosting providers in responsibilities under the data protection framework under the notion of co-controllers.[77]

---

68 ECD, recital 47 and 48 respectively.
69 Case C-360/10 *SABAM*; Case C-70/10 *Scarlet v. Sabam* EU:C:2011:771.
70 Case C-324/09 *L'Oreal and Others*, para 139 ff.
71 Case C-314/12 *UPC Telekabel Wien*.
72 Case C-484/14 *Tobias McFadden*, para 90 ff.
73 Case C-18/18, *Glawischnig-Piesczek*, para 44 ff.
74 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, Art.17(8).
75 Directive 2010/13 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), OJ [2010] L 95/1, as amended by Directive 2018/1808, Art.28a(3).
76 See for more, Peguera (2016).
77 See Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein* EU:C:2018:388, and broadly: Mahieu et al. (2019).

2.3. Developments in EU legislation

Since the adoption of the e-commerce Directive in 2000, many new rules and enforcement institutions relating to the provision of Information Society Services have been adopted by the EU legislators.[78]

Some of those rules target specific categories of ISS, in particular,

- The *Network and Information Security (NIS) Directive* imposes specific security requirements on *online market places*[79] such as eBay or Amazon, on *online search engines*[80] such as Google Search or Qwant and on *cloud computing service*[81] such as Microsoft Azure;
- The revised *AVMSD* imposes specific obligations to tackle harmful and illegal content on *Video Sharing Platforms* such as YouTube;[82]
- The *European Electronic Communications Code (EECC)* regulates *number-independent Interpersonal Communications Services* such as Skype, WhatsApp or Gmail;[83]
- The *DSM Copyright Directive (DSMD)* imposes specific obligations to ensure copyright compliance on *Online Content Sharing Service providers* like video- or picture-sharing platforms;[84]
- The *Platform-to-Business Regulation* imposes specific transparency obligations on Online Intermediation Services such as online e-commerce marketplaces, app stores and online social media services[85] and on *Online Search Engines*.[86]

---

78 For a review of all the rules adopted between 2014 and 2019 in the context of the Digital Single Market, see de Streel and Hocepied (2019). For a review of the evolution of the EU e-commerce rules since the adoption of the ECD, see de Streel, Buiten and Peitz (2018: 13-32).

79 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, OJ [2016] L 194/1, Art.4(17) defines *online marketplace* as 'a digital 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.'

80 NIS Directive, Art.4(18) defines *online search engine* as 'a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.'

81 NIS Directive, Art.4(19) defines *cloud computing service* as 'a digital service that enables access to a scalable and elastic pool of shareable computing resources.'

82 AVMSD 2010/13, as amended by Directive 2018/1808, Art.1(aa) defines *Video-Sharing Platform Service* as 'a service as defined by Art.s 56 and 57 TFEU, where the principal purpose of the service or of a dissociable Section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks (…) and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing.'

83 Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ [2018] L 321/36, Art.2(5) defines *number-independent Interpersonal Communications Services* as 'a service normally provided for remuneration 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(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.'

84 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, OJ [2019] L 130/92, Art.2(6) defining *Online Content-Sharing Service Provider* as: 'a provider of an information society service of which the 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, which it organises and promotes for profit-making purposes.'

85 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, OJ [2019] L 186/55, Art.2(2) defines *Online Intermediation Service* as as 'services which meet all of the following requirements: (a) they constitute Information Society Services (…); (b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers.'

86 Platform to Business Regulation, Art.2(5) defines a *Online Search Engine* as 'a digital 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.'

Other rules are more general and apply to providers of all types of services in order to improve,

- The fundamental freedoms of movement in the EU;
- Consumers and users and data protection;
- Cooperation between Member States or regulatory mechanisms.

All those new rules do not undermine the fundamental logic and principles of the ECD but complement each of its four pillars.[87]

2.3.1. Internal Market rules

One of the most important EU laws that has been adopted since the enactment of the e-commerce Directive is undoubtedly the ***Services Directive*** in 2006.[88] The Directive follows the same logics than the ECD, albeit in a more modest manner as it covers a much broader scope of services. Indeed, the Services Directive limits the possibility of the Member State to impose prior authorisation schemes, affirms the country of origin, harmonises some obligations to increase user's protection and encourages cooperation between Member States, which is indispensable for the acceptance and the functioning of the 'country of origin' principle. Thus, the Services Directive nicely complements the ECD and sets up cooperation mechanisms between Member States which may be relied upon in the context of ISS.

In addition, the ***Transparency Directive***, which defines the Information Society Service and the scope of the ECD, has been consolidated in 2015.[89] However, the material definition of the ISS has not been changed.[90]

2.3.2. Protection of users

Another important evolution of EU law has been the strengthening of consumer protection, in particular with the adoption of the ***Unfair Commercial Practices Directive*** in 2005[91] and the ***Consumer Rights Directive*** in 2011.[92]

In 2019, both Directives were revised to improve their enforcement and better adapt the protection of consumer in the digital age[93] while a new Directive protecting the consumer of ***digital content*** was also adopted.[94] Those Directives, which are of maximum harmonisation, complement the ECD[95] and strengthen the protection of the users of ISS when they act as consumers, i.e. for purposes which are outside their trade, business, craft or profession.

---

87 The relationship between many of those new rules and the ECD is analysed in Commission Staff Working Document of 11 January 2012, Online services, including e-commerce, in the Single Market, SEC(2011) 1641.

88 Directive 2006/123 of the European Parliament and of the Council of 12 December 2006 on services in the internal market, OJ [2006] L 376/36.

89 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, OJ [2015] L 241/1.

90 Case C-390/18, *Airbnb Ireland*, para.43.

91 Directive 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ [2005] L 149/22.

92 Directive 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, OJ [2011] L 304/64.

93 Directive 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13 and Directives 98/6, 2005/29 and 2011/83 of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ [2019] L 328/7.

94 Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ [2019] L 136/1.

95 See Commission Staff Working Document of 25 May 2016 on Guidance on the implementation/application of the Directive 2005/29 on Unfair commercial practices, SWD(2016) 163, pp. 22 and 119-124.

Indeed, on the basis of the EU consumer acquis, the National Consumer Protection Authorities took several actions, often coordinated at the EU level within the Consumer Protection Cooperation Network, to force online platforms such as the social media platforms (Facebook, Twitter), the app stores (Google Play and Apple iTunes), the hosting platforms (Airbnb and Booking) to change the terms of services to be more transparent and fairer towards the EU consumers.[96] During the Covid-19 crisis, the CPC and the Commission adopted in March 2020 a Common Position, based on the Unfair Commercial Practices Directive and the ECD, to stop scams and tackling unfair business practices on online platforms.[97]

The protection of some business users has also been recently strengthened with the adoption of the ***Platform-to-Business Regulation*** in 2019. This Regulation imposes a series of transparency obligations in favour of the business users when dealing with providers of ISS offering intermediation or search services[98] and impose the establishment of specific enforcement mechanisms such as internal complaint-handling system, mediation and collective actions.[99]

With regard to the specific and important issue of **commercial communications or advertising**, those new general rules increase transparency requirements. In addition, some specific rules applicable to specific types of ISS impose stricter requirements. This is the case of the revised AVMDS imposing specific requirements for video sharing platforms.[100] Rules differ according to whether the commercial communications are marketed, sold or arranged by the video sharing platforms directly[101] or by others.[102] Moreover, the AVMSD prohibits video sharing platforms from processing the personal data of minors for commercial purposes such as direct marketing, profiling and behavioural advertising when trying to protect minors (by deploying parental control or rating systems). This rule shows that there is a special need to protect minors regarding the use that can be made of their personal data by platforms, beyond the level of protection already afforded under the GDPR. Nevertheless the harmonisation of the new AVMSD for commercial communications is limited to video-sharing platforms.

Next to consumers and users protection rules, the rules on data protection have been revised and strengthened in 2016. The new ***General Data Protection Regulation (GDPR)***[103] carries over the main rights of the data subjects of the previous Privacy Directive and creates new ones, in particular to improve the right to be delisted, data mobility and explainability of automated decisions.

---

96 See the CPC website: https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/consumer-protection-cooperation-network_en#i

97 https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/scams-related-covid-19_en. This concerned in particular the following online platforms: Allegro, Alibaba, Amazon, Bing, Cdiscount, Ebay, Facebook, Google, Rakuten and Yahoo.

98 P2B Regulation, arts.3-10.

99 P2B Regulation, arts.11-17.

100 AVMSD, Art. 28b(2).

101 In this case, the video sharing platforms need to comply with the qualitative requirements applicable to linear and non-linear audio-visual media service providers: AVMSD, Art. 9 (1).

102 In this case, the video sharing platforms should take appropriate measures to ensure that these rules are complied with taking account the limited control they exercise over those commercial communications. At the very least they should have a functionality for users who upload user-generated videos to declare whether such videos contain audio-visual commercial communications as far as they know or can be reasonably expected to know and inform them that the qualitative rules should be respected.

103 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), OJ [2016] L 199/1.

2.3.3. Liability rules

The ECD forms the cornerstone of the regulation of illegal content in the online environment. Since its adoption, technology and markets have changed substantially. Some online platforms have become very large thanks to direct and indirect network effects,[104] hence the harm caused by illegal material is more massive as they affect many more users.

At the same time, the financial, technological and human capacities of the platforms to prevent and remove such illegal material have also expanded while more effective automated techniques for identifying illegal content have become available, decreasing the costs for victims and online hosting platforms to prevent harm caused by illegal material.[105] These evolutions triggered a call to increase the responsibility of the online platforms.[106] Responding to this call the EU institutions did not change the ECD but clarified some of the provisions in order to step-up the fight against illegal material and, in parallel, developed stricter specific rules for some types of material which are particularly harmful (as summarised in Table 1 below).

First, the **Commission clarified the ECD by adopting a Communication in 2017, followed by a Recommendation in 2018**.[107] These two instruments aim to improve the effectiveness and transparency of the Notice-and-Takedown process between the users and the platforms, stimulate preventive measures by online platforms, and increase cooperation between providers of hosting services and the specific stakeholders (in particular of users, trusted flaggers and public authorities). Yet, although Member States should take into the utmost account a Recommendation, this legal act is not legally binding.[108]

Secondly, the **baseline regime of the ECD has been complemented for particularly harmful illegal material by sectoral rules and co/self-regulatory measures** increasing the actions against those types of content. From the legislations which were adopted or considered over the years at the EU level, the following are worth mentioning,

- ***Directive combatting child sexual abuses*** (2011) obliges Member States to take the necessary measures to ensure the prompt removal of, or with appropriate safeguards block access to, web pages containing or disseminating child pornography.[109] On that basis, Member States have implemented Notice-and-Takedown procedures through national hotlines, to which Internet users can report child sexual abuse material that they find online;[110]
- ***Directive combatting terrorism*** (2017) obliges Member States to take the necessary measures to ensure the prompt removal of, or with appropriate safeguards block access to, online content constituting a public provocation to commit a terrorist offence;[111]

---

104 Martens (2016).

105 For an review of those techniques and their costs, see Ecorys (2016, pp. 40-54); ICF, Grimaldi Studio Legale, and 21c Consultancy (2018, pp. 138-145).

106 Communication from the Commission of 25 May 2016, Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe, COM(2016) 288.

107 Communication of the Commission of 28 September 2017, Tackling Illegal Content Online. Towards an enhanced responsibility for online platforms, COM (2017) 555 and Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, OJ [2018] L63/50.

108 TFEU, Art.288. Case C-16/16P *Belgium v. Commission* EU:C:2018:79.

109 Directive 2011/93 of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ [2011] L 335/1, Art.25.

110 Report from the Commission of 16 December 2016 assessing the implementation of the measures referred to in Art. 25 of Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography, COM(2016) 872. INHOPE is the umbrella organisation for the hotlines.

111 Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ [2017] L 88/6, Art.21.

- In addition, a proposal for a ***Terrorist Content Regulation*** is currently being negotiated,[112] which covers preventive duties and the process of content removal of the terrorist content by the hosting providers.[113] It prescribes a removal of terrorist content within one hour.[114] It also includes rules concerning complaint mechanisms, transparency obligations and data retention;
- ***General Data Protection Regulation (GDPR)*** (2016) includes a special rule concerning search engines and their obligation to delist content from the search results (also known as 'right to be forgotten'). In addition, the new case-law of the Court of Justice gives providers data protection responsibilities concerning the hosted content under some circumstances;[115]
- ***Audio-visual Media Services Directive (AVMSD)*** revised in 2018 regulates video-sharing platforms hosting content over which they do not have editorial responsibility, like user-posted videos, in the area of harmful content for minors and terrorist, racist/xenophobic content, child pornography and hate speech content for general public. Such platforms are obliged to take preventive measures concerning the organisation of the content and not to the content as such.[116] This includes measures like easy-to-use flagging systems, effective complaint systems, parental control, verification systems and transparency obligations.[117] None of these measures may, however, lead to any ex-ante control measures or upload-filtering of content which do not comply with the prohibition of general monitoring measures of the ECD. Although, the Member States might adopt stricter preventive measures than those listed in AVMSD,[118] these are still subject to the same limitations of the ECD. In addition, the AVMSD includes some general requirements[119] concerning user's disputes over incorrect removal of content;
- ***DSM Copyright Directive*** *(DSMD)* adopted in 2019 regulates Online Content Sharing Service providers, like video- or picture-sharing platforms, and their responsibility for licensing of content posted by their users. DSM Directive complements the *Intellectual Property Enforcement Directive*.[120] By default, the providers have to engage in "best efforts" to obtain licenses for content potentially posted by their users. If such licenses are missing, though "best efforts" to obtain them can be demonstrated, they are liable for violation of copyright or neighbouring rights, *unless* they take-down material upon notification, and prevent its re-appearance on the service (if given the relevant information in both cases).[121] The preventive duties have to comply with the general monitoring prohibition, although such obligation is an extension of Art. 15 ECD requirement, since Online Content Sharing Services Providers are of 'active' nature.[122] In addition the DSMD includes a number of unspecified safeguards against incorrect removal of content by the providers, which are absent in the ECD framework;

---

112 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.
113 See Art. 3-6 of the Proposal.
114 Art. 4(2) of the Proposal.
115 See Section 3.2; see on the relationship, Peguera M. (2016).
116 AVMSD, recital 48.
117 AVMSD, Art.28a(3).
118 AVMSD, Art.28a(6).
119 AVMSD, Art. 28a(3)(j);(7);(8).
120 Directive 2004/48 of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ [2004] L 195/16.
121 DSMD, Art.17(4).
122 See on the reason why active services are not covered by Art. 15 ECD in Section 2.2.3.

In addition, the European Commission encouraged self- and co-regulation in the area, such as,

- **Counterfeit goods** with the adoption of a *Memorandum of Understanding (MoU) on illegal counterfeiting* in 2011 between rights owners, Internet platforms and associations to improve Notice-and-Takedown and enhance preventive measures taken by rights owners and online intermediaries, increase cooperation and better fight against repeated infringements; a revised version was signed in May 2016 to include Key Performance Indicators in order to facilitate its monitoring; [123]
- **Child sexual abuses** with the establishment of the *Alliance to Better Protect Minors Online* in 2017 composed of actors from the entire value chain (devices manufacturers, telecoms, media and online services used by children) 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); [124]
- **Terrorist content** with the establishment of a *Multi-Stakeholders Forum* in 2015 between the EU Interior Ministers, the major internet companies (such as Facebook, Google, Microsoft and Twitter), Europol, the EU Counter Terrorism Co-ordinator and the European Parliament[125] to address the misuse of Internet by terrorist groups and to reduce accessibility to terrorist content online; the Forum led to an efficient referral mechanism in particular with the EU Internet Referral Unit of Europol, a shared database of hashes with more than 200,000 hashes of terrorist videos and images;
- **Hate speech** with the adoption of an *EU Code of Conduct on Countering Illegal Hate Speech Online* in 2016 by the main Internet platforms (such as Facebook, Microsoft, Twitter, YouTube, Instagram, Dailymotion, Snapchat or Jeuxvideo); [126]
- **Online disinformation and fake news**: with the adoption of a *Code of Practice on Disinformation* in 2018 by online platforms (Facebook, Google, Twitter, Mozilla and Microsoft), advertisers and the advertising industry to better tackle illegal but also harmful fake news and online disinformation. [127]

[123] See https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en

[124] See https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online. For an evaluation of such Alliance, see Ramboll (2018). Previous initiatives were: a CEO Coalition in 2011: 'Self-regulation for a Better Internet for Kids' https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids; an ICT Coalition for Children Online in 2012: http://www.ictcoalition.eu.

[125] Commission Press release of 3 December 2015, IP/15/6243.

[126] Code of Conduct of May 2016 on Countering Illegal Hate Speech online: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.

[127] EU Code of Practice of October 2018 on Disinformation: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

Table 1: EU rules against online illegal material

Type of illegal content	Hard-law	Soft-law	Co/self-regulation	Hard-law
BASELINE All types of illegal content online	Directive 2000/31 e-commerce 1	Communication 2017 Illegal Content Online - Recommendation 2018/334 Illegal Content Online		
IP violation	Directive 2019/790 Copyright in the Digital Single Market - Directive 2004/48 on Enforcement of Intellectual Property Rights			Memorandum of Understanding on Counterfeit Goods Online (2011-2016)
Child sexual abuse material	Directive 2011/93 Child Sexual Abuse			- CEO Coalition (2011) - ICT Coalition for Children Online (2012) - Alliance to Better Protect Minors Online (2017)
Terrorist content	- Directive 2017/541 Terrorism - Proposal Regulation Terrorism Online Content	- Recommendation 2018/334 Illegal Content Online		EU Internet Forum (2015)
Hate speech	- Directive 2010/13 Audio-visual Media Services as amended by Directive 2018/1808 in case of video-sharing platforms			- Code of Conduct on Illegal Hate Speech Online (2016)
Disinformation and fake news				- EU Code of Practice on Disinformation (2018)

This increasingly fragmented landscape shows that the EU legislator is pursuing the strategy of sector-specific measures. In each of these instruments, it has to separately define the potential preventive duties, notice and takedown procedure and safeguard mechanisms, including the complaint mechanisms. The main focus is clearly on the hosting service providers. At the same time, **most of these initiatives build on top of the e-commerce Directive, and try to supplement the lack of specificity** on its side. Even the DSM Directive does not necessarily contradict the ECD as it applies to a subset of more active hosting services.[128] However, this depends on the future interpretation of ECD's requirement of passive/active services, and DSMD's definition of Online Content Sharing Services providers. If the changes to the ECD's requirement are made in the future, DSMD is already worded in a way which treats it as *lex specialis*. In fact, by extending the general monitoring prohibition, DSMD further borrows from the ECD.

2.3.4. Enforcement mechanisms

To facilitate the **cooperation and mutual assistance between the authorities of the Member States**, several mechanisms and networks have been set up since 2000. The main ones are:

- The establishment of the ***expert group on electronic commerce*** in 2005 which is composed of the different national contact points and chaired by the Commission;[129] this expert group has been useful in discussing the derogation to the Internal Market Clause, codes of conduct, liability of intermediaries and national Notice-and-Takedown procedures;[130]
- The establishment of the ***Consumer Protection Cooperation (CPC) Network*** in 2006 composed of the national consumer protection authorities which was strengthened in 2017;[131] this network has taken several actions, through sweeps or coordinated actions, to ensure that online providers, which often offer their services cross-border, comply with EU consumer protection legislation.[132] As already noted, the CPC Network took several coordinated actions against digital platforms and the strengthening of the Network proved to be very useful in tackling online scams and unfair business practices during the Covid-19 crisis;
- The establishment of the ***Internal Market Information (IMI) System*** which is a multilingual secure online application to facilitate communications and support cooperation between the

[128] DSMD, Art.2(6) provides that: "'online content-sharing service provider' means a provider of an information society service of which the 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, *which it organises and promotes for profit-making purposes*.' (emphasis ours).

[129] 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.

[130] Commission Staff Working Document of 11 January 2012, Online services, including e-commerce, in the Single Market, SEC(2011) 1641, p.23.

[131] Regulation 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Regulation on consumer protection cooperation), as amended. Now replaced by Regulation 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation 2006/2004, OJ [2017] L 345/1.

[132] All those actions can be found on the website of the CPC Network is at:
https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/consumer-protection-cooperation-network_en#i. A "sweep" is a set of checks carried out on websites simultaneously to identify breaches of EU consumer law in a particular sector. The Commission Staff noted that the increasing reliance on the CPC Network for matters related to the ECD could make the derogation to the Internal Market Clause less necessary: Commission Staff Working Document of 11 January 2012, Online services, including e-commerce, in the Single Market, SEC(2011) 1641, p.22.

competent authorities of the Member States.[133] Between 2013 and 2019, Member States exchanged 139 requests and 105 notifications related to the ECD via the IMI System.[134]

With regard the **alternative enforcement mechanisms**, new horizontal legislations have been adopted regarding *Alternative Dispute Resolution (ADR)*,[135] and *Online Dispute Resolution (ODR)*[136] for consumers. Some more recent EU initiatives applicable to specific Information Society Service providers also refer to the availability of out of court redress mechanisms for the settlement of specific disputes (e.g. disputes between users and video sharing platforms in the AVMS Directive).[137] The danger with the adoption of these sectorial EU legislations is that when Member States adopt implementing legislation, they too adopt piecemeal laws which would lack overall coherence, leading to complex situations for users, platforms and oversight bodies.

Also, the Commission has developed, by open consultation, ***principles for better self-and co-regulation*** that have been tested by pilot Community of Practice.[138] 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.

Co-regulation has become an efficient way to address some of the weaknesses of self-regulation (in particular biases, lack of enforcement) and of regulation per se (in particular enforceability difficulties, rigidity), while preserving a certain degree of public oversight over key aspects of policy intervention. Co-regulation has been particularly effective in some Member States (in particular the Netherlands and Germany) and in some areas (in particular the protection of minors and advertising). The revised AVMSD Directive is also stressing the need to encourage self and co-regulation in relation video-sharing platforms, where the onus of ensuring the protection of users lies primarily with the platforms, whereas the regulator's role could be limited to check that the measures taken by the platform are appropriate.[139]

2.4. Developments at national level

Although the ECD aimed to increase legal certainty and harmonisation regarding the liability of the online intermediaries for the illegal content they host, some divergences remain across the Member States. There are two areas which have seen the most friction on the national level.

First, some national courts construe the notion of **passive hosting** providers differently.

There is a growing case-law before the European Court of Human Rights which shows that many national courts arguably misapply the ECD in various ways.[140]

---

[133] Regulation 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC (the IMI Regulation), OJ [2012] L 316/1, as amended by Directives 2013/55, 2014/60, 2014/67 and Regulations 2016/1191, 2016/1628 and 2018/1724. Art.29(3) of this Regulation provides that IMI should be used as pilot project for the implementation of the derogation procedure foreseen by Art.3 of the ECD.

[134] See: https://ec.europa.eu/internal_market/imi-net/statistics/2019/08/e-commerce/index_en.htm.

[135] Directive 2013/11 of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation 2006/2004 and Directive 2009/22 (Directive on consumer ADR) OJ [2013] L 165/63.

[136] Regulation 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes (Regulation on consumer ODR), OJ [2013] L 165/1.

[137] AVMSD, Art.28b(7).

[138] Those principles are available at : https://ec.europa.eu/digital-single-market/en/best-practice-principles-better-self-and-co-regulation.

[139] AVMSD, Art.28b(4). See Capello et al. (2019).

[140] ECtHR, *Delfi AS v. Estonia* [GC] (App no 64569/09) ECHR 16 June 2015; *Magyar Tartalomszolgáltatók Egyesülete and Index.Hu Zrt v. Hungary* (App no 22947/13) ECHR 02 February 2016.

In the past, many service providers that filed complaints before the European Court of Human Rights for violation of their freedom of expression should have arguably been able to benefit from the hosting safe harbour on the national level. However, activities like hosting of user-comments under news Art.s were seen as too active, and thus outside of the ECD framework.[141]

Second, although some Member States adopted variations of the **Notice-and-Takedown procedure** in their national laws in the implementation stage,[142] these were never tested before the Court of Justice for their (in) effectiveness. Several Member States adopted or consider adopting new rules, which would prescribe specific deadlines for hosting providers. **Adoption or proposals of recent laws in the Member States, in particular regarding hate speech, further increased the risks of Internal Market fragmentation**.

For instance in 2017, Germany adopted the *Network Enforcement Act (NetzDG)* which requires in particular online platforms with more than two million subscribers in Germany to set-up a system for users to complain against hate speech and to remove or block access to within 24 hours from the user's notification; for content that is not obviously illegal, platforms have seven days to remove it or must delegate a self-regulatory body to assess it. In case of repeated incompliance they face fines up to €50m.

Currently, France is debating a draft law to fight online hate speech which would impose the removal of obviously illegal content within 24 hours from the user's notification as well as other complementary obligations (such consumer friendly notification process and transparency reports) under the supervision of the French media regulator. This draft law has been notified to the Commission under the Transparency Directive and the Commission has sent to France several critical observations regarding the compatibility of the draft law with the Art.s 3, 14 and 15 ECD.[143]

[141] Ibid.

[142] See for the overview, ICF, Grimaldi Studio Legale, and 21c Consultancy (2018, pp. 18-108 and Annex); Kuczerawy (2018).

[143] Commission Decision of 22 November 2019, *Notification 2019/412/F, Loi visant à lutter contre les contenus haineux sur internet : Emission d'observations prévues à l'Art. 5, paragraphe 2, de la directive 2015/1535*, C(2019) 8585.

3. EVALUATIONS OF THE DIRECTIVE AND IMPACT ON THE INTERNAL MARKET

KEY FINDINGS

The European Commission did **three main waves of evaluation** of the E-commerce Directive and more generally of the EU rules and policies on digital platforms.

In the first evaluation which took place in **2003** when the Directive was about to be transposed by the Member States, the Commission observed **positive trends**, in particular a reduction in Court proceedings on the liability of digital platforms and overall satisfaction of the country of origin principle.

In the second evaluation which took place in **2011-2012**, the Commission found that the **principles and the rules of the ECD were sound**, but that some improvements were needed, in particular regarding the notice-and-takedown systems.

In the third evaluation which took place in **2016-2017**, the Commission found again that the principles and the rules of the ECD were sound. However, the Commission observed the **increasing importance of online platforms and the new risks of digital single market fragmentation**. This led to three-pronged strategy: (i) adapt sectoral hard-law when there is a specific problem; (ii) give more guidance on the interpretation of the less clear provisions of the e-commerce Directive, in particular regarding the notice-and-takedown and the reliance on voluntary preventive measures; and (iii) encourage coordinated EU-wide co and self-regulation for the illegal materials which are particularly harmful.

Academic studies identified that the underlying **notice and takedown framework generally is exposed to the following trends**: the quality of notifications sent to the providers is often very low (at least in some areas); there is a diverging quality of such notifications among different notifiers; the notifications are increasingly out-sourced to professional companies; increasingly, the notifications are sent by algorithms, and not humans; providers tend to over-remove content to avoid liability and save resources; they equally employ technology to evaluate the notifications; the affected users who posted content often do not take action.

The E-commerce Directive is one of the cornerstones of the Digital Single Market which, with the increasing digitisation of the economy and the society, should now underpin the whole internal market project.

3.1. Existing evaluations

3.1.1. Evaluations by the European Commission

Since the adoption of the e-commerce Directive in 2000, the European Commission conducted three main evaluations of the Directive and its relationship with the other EU legal instruments applicable to online platforms.

(i) 2003 Evaluation: First Implementation Report

In its first implementation Report, the Commission recognised that the impact of the ECD was **too early** to be evaluated given the lack of experience with the Directive.[144] However, the Commission observed **two positive elements**. First, the ECD appeared to be successful in reducing court proceedings and hence legal uncertainty, in particular as regards liability of online intermediaries. Second, the only complaints received at the time by the Commission from companies engaged in cross-border online activities concerned matters excluded from the scope of application of the Directive or from the application of the Internal Market Clause, such as online gambling, suggesting that, otherwise, the ECD was a success. [145]

(ii) 2011-2012: e-commerce Action Plan

Within the Digital Agenda for Europe,[146] the Commission adopted in 2012 an important *E-commerce Action plan* with 16 policy actions.[147] In that context, the Commission did a thorough economic and legal evaluation of the ECD based on a public consultation and several independent studies.

The economic evaluation indicated that the **development of e-commerce could generate an overall gain for consumers of around €204 billion** (1.7% of European GDP at the time) if e-commerce reached 15% of retail sales and if the obstacles to the Single Market were removed.[148]

The legal evaluation indicated that the principles and the **rules of the ECD were sound** and did not need to be revised.[149] However, the Commission identified several avenues for improvements,

- First, the cooperation between Member States authorities in implementing the ECD needed to be strengthened, by improving the notification of derogation to the Internal Market Clause, in particular using the IMI System, and by strengthening the dialogue within the e-commerce expert group;
- Second, the provisions of the ECD on the liability of intermediaries and general monitoring prohibition needed to be clarified given the divergences in national laws and case-law and additional clarifications on Notice-and-Takedowns process needed to be given;
- Third, additional EU laws needed to be adopted and coordinated with the ECD to stimulate national and cross-border e-commerce, in particular regarding consumer and data protection, transparency, non-discrimination, contract and e-identification, e-payment, parcel delivery and VAT.

(iii) 2016-2017: Online Platforms

Within the *Digital Single Market Strategy*,[150] the Commission adopted successively in 2016 and in 2017 two important policy Communications on online platforms with the objectives, among others, to increase the responsibility as well as the transparency and fairness of the platforms.[151]

---

144 Report of the Commission of 21 November 2003 on the application of Directive on electronic commerce, COM(2003) 702, p.19.
145 *Ibidem*, pp. 19-20.
146 Commission Communication 'A Digital Agenda for Europe' COM(2010) 245.
147 Communication from the Commission of 11 January 2012, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM(2011) 942. For a first follow-up, see Commission Staff Working Document of 23 April 2013, E-commerce Action plan 2012-2015: State of play 2013, SWD(2013) 153.
148 Commission Staff Working Document of 11 January 2012, Bringing e-commerce benefits to consumers, SEC(2011) 1640.
149 Commission Staff Working Document of 11 January 2012, Online services, including e-commerce, in the Single Market, SEC(2011) 1641.
150 Communication from the Commission of 6 May 2015, A Digital Single Market Strategy for Europe, COM(2015)192.
151 Communication from the Commission of 25 May 2016, Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe, COM(2016) 288, pp.7-13 and Communication from the Commission of 10 May 2017 on the Mid-Term Review on the implementation of the Digital Single Market Strategy, COM(2017) 228, pp. 7-9.

In that context, the Commission did a thorough assessment of the role of online platforms[152] and their regulatory framework based on a series of public consultations[153] and independent studies.

Specifically with regard the ECD, most of the Commission assessment **focussed on the liability regime**, its harmonisation across the EU and its effectiveness in tacking illegal content online. According to the 2016 Commission public consultation,[154] '[a] majority of the respondents stands behind intermediary liability principles of the e-commerce Directive, but also demands some clarifications or improvements'. A significant proportion of respondents who criticised the Directive complained about the national implementations rather than the EU law itself. The stakeholders broadly supported the horizontal nature of the Directive, but demanded a differentiated approach on Notice-and-action; by adjusting or improving the practice of take-down for specific types of content, such as hate-speech, terrorist content, child abuse material, copyright infringements, etc.

Regarding the functioning of ECD rules, the most attention was paid to the hosting safe harbour (Art. 14), in particular its concept of 'passive hosting'. The concept was criticised for not being entirely clear, and for divergent national interpretations. As regards the missing components, an '[o]verwhelming majority of respondents supported the establishment of a counter-notice mechanism (82.5%), i.e. possibility for content providers to give their views to the hosting service provider on the alleged illegality of their content'.[155] The consultation also recorded a significant support for more transparency on the intermediaries' content restriction policies.[156] On the side of preventive duties, a majority of intermediaries reported that they do put in place voluntary or preventive measures to remove certain categories of illegal content from their system beyond what was required by the legal framework. In the consultation, only 36.1% of respondents reported a need to impose specific duties of care for certain categories of content.

3.1.2. Other evaluations

There are very few academically sound evaluations of the ECD. Part of the problem is that the Directive deals with the vast range of services in many different areas.

With regard to the **economic benefits of e-commerce** in general, the EPRS (2019, p. 56) notes that a JRC study[157] estimated that sound digital policies could bring an overall gain for the EU economy in the long run between 0.44% and 0.82% of GDP considering the potential efficiency and competition effects.

This means that, after full implementation of the appropriate policies to complete the Digital Single Market, the EU economy could be expected to enjoy up to €110 billion of additional GDP per year. Marcus et al. (2019) have identified, on the basis of the Commission ex ante assessments, some €177 billion in potential annual economic gains (in current euro) from full implementation of the legislative measures enacted in 2014-2019 in the context of the Digital Single Market, corresponding to 1.2% of 2017 GDP.

With regard to the **liability of platforms**, some of the empirical studies looked at the question of removal of the illegal content. However, most of them are copyright-centred, and not necessarily localised to only EU markets. The other problem is that in the online environment, where many firms

[152] Commission Staff Working Document of 25 May 2016, Online Platforms, SWD(2016) 172. Also Martens (2016).
[153] The results of the public consultation could be found at: https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud. For an qualitative analysis of the results, see Gawer (2016) and TILT (2016).
[154] TILT (2016, p. 4).
[155] Ibid, p. 5.
[156] Ibid, p. 6.
[157] Christensen, Conte, Di Pietro, Lecca, Mandras and Salotti (2018).

are operating globally with global version of products, the broadly drafted EU rules sometimes could give a way to more prescriptive rules from the US (especially in copyright law). Therefore, even the value of the national experiments could have been limited on the global stage.[158]

Among the academic studies, the studies of the ecosystem fit into several categories: (1) interviewing notifiers, providers and users;[159] (2) experimental upload of content,[160] (3) analysis of transparency reports or data sets shared publicly by providers, such as *Lumen* data[161], (4) tracking of the public availability of the content over a pre-set period[162] and (5) experimental testing of redesigns of ECD.[163] The studies so far show a number of global trends, which are not always localized to the European setting, namely,

- the quality of notifications sent to the providers is often low (at least in some areas);
- there is a diverging quality of such notifications among different notifiers;
- the notifications are increasingly out-sourced to professional companies;
- increasingly, the notifications are sent by algorithms, and not humans;
- providers tend to over-remove content to avoid liability and save resources;
- they equally employ technology to evaluate the notifications;
- the affected users who posted content often do not take action.

These phenomena are party to be attributed to the ECD, although they were not caused by the Directive, rather than by the lack of legal of provisions tackling such challenges.

3.2. The ECD as the cornerstone of the Internal Market

As put by the European Commission, the **Internal Market Clause**, which states that the Member States may not restrict the freedom to provide Information Society Services from another Member State, is the **cornerstone of the Digital Single Market**.'[164] Indeed, this clause which clarifies and operationalizes the fundamental freedoms of the TFEU, has been key for the development of cross-border e-commerce to the benefit of EU consumers and platforms alike.

As explained above, the implementation of such clause has been firmly upheld by the Court of Justice and most commentators agree that the ECD has greatly contributed to the free movement of the Information Society Services.

In addition, the **common liability exemption rules allow the firms to more easily scale up** on the digital single market. Although far from constituting uniform rules, they give companies basic reassurances concerning the operation of their business in dealing with third-party content, and to stakeholders in enforcement of their rights. They also provide a common vocabulary for European judicial discourse. The benefits in terms of approximating the liability framework can be best seen when compared with largely the non-harmonised preventive measures.[165] Despite diverging national doctrines used for establishing liability, the debate often concentrates on the key issues of the EU law,

[158] See Husovec (2019).
[159] Urban et al. (2017a)
[160] Perel and Elkin-Koren (2017); Sjoera (2004).
[161] Urban and Quilter (2006); Urban et al. (2017a) and (2017b); Seng (2014) and (2015); See https://www.lumendatabase.org/.
[162] Erickson and Kretschmer (2018).
[163] Fiala and Husovec (2018).
[164] Communication from the Commission of 11 January 2012, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM(2011) 942, p.5.
[165] The exception being intellectual property law, Husovec (2017a).

in particular concerning the hosting safe harbour. Although the national courts are far from consistent in applying these rules, the preliminary references to the Court of Justice facilitate the dialogue. This creates a platform for basic coordination of the rules and judicial cooperation. In some areas, like intellectual property law, the litigation become the main engine of defining the liability of the service providers.

The open-ended framework of the ECD also allows experimentation on many issues, which facilitates the learning among the experts. Again, in intellectual property law which is responsible for most of the case-law related to liability rules, judges and legislators took the opportunity to learn from each other. For instance, website blocking measures adjudicated in the UK informed litigation in many other EU Member States, and German-style preventive duties known as 'disturbance liability' inspired other jurisdictions.

Taking a broader scope, de Streel and Hocepied (2019) explained that the **ECD is key part of the Digital Single Market which is composed on six main building blocks**. The two first blocks relate to the digital services used by European consumers and citizens: the e-commerce and online platforms and the e-government services. The three successive blocks are horizontal and necessary to ensure the development of and the trust in private and public digital services; they relate to data and AI, security and the specific consumer protection for the digital era. Finally, the last block relates to the infrastructures on which the digital applications are provided: the electronic communications networks and services.

Each block has been improved with the adoption of many new rules and policies in the context of the Digital Single Market Strategy that the Commission launched in 2015. On the basis of the impact assessments done by the Commission, Marcus et al. (2019) calculated that some **€177 billion in potential annual economic gains** from full implementation of the legislative measures enacted or expected to be enacted, corresponding to 1.2% of 2017 GDP .

In the future as the economy and the society are increasingly digitised, the **Digital Single Market should become more and more the digitised single market**. As new digital technologies are general-purpose technologies which permeate all the sectors of the economy, it is appropriate to digitize the four freedoms and all the sectors of the single market instead of developing a specific strategy for digital sectors.[166]

[166] As suggested by several Think-Tanks such as Bruegel (2019), CERRE (2019), Lisbon Council (2018).

4. OUR ASSESSMENT AND RECOMMENDATIONS

KEY FINDINGS

The definition of the **Information Society Service**, which determines the scope of the ECD, proves to be **robust over time** and applicable to new business models. The concerns raised by some that the no prior authorisation rule applicable to ISS severely limits the competence of the Member States to regulate the underlying services intermediated by **collaborative economy** platforms, such as transport or hosting, have proven to be unfounded.

The **Internal Market Clause is one of the greatest successes** of the e-commerce Directive. To be accepted and effective, such clause requires trust between Member States that the regulation in the country of origin is sufficiently protective and effectively enforced. In turn, this requires the EU harmonisation of the main protection rules and effective cooperation between national authorities. Fortunately since the adoption of the ECD, both have increased. Thus, in any review of the ECD, **the country of origin should absolutely be maintained while the cooperation between Member States could be strengthened** and better organised in order to make the procedure more efficient and rapid, in particular between the country of origin and the country of destination where the provider is offering its services. Moreover, the ECD and its Internal Market Clause, could also be **extended to cover the online platforms which are not established in the EU** but provide their services to EU customers, for instance by requiring the designation of a representative in the EU.

The criticism of the Directive's **liability rules** can be grouped as follows: (1) the Directive lacks sufficient safeguards to prevent violations of fundamental rights, in particular freedom of expression; (2) the Directive does not envisage that notifications may be sent by robots and fails to incentivise the quality of sent and reviewed notifications; (3) the Directive does not prevent fragmentation due to diverging application of the passivity criterion by the national courts; (4) the Directive fails to cover hyperlinking and search engines and other new services; (5) the Directive only serves as a limit and not as a comprehensive tool of removal of illegal content. Each of these points demands a response when updating the ECD.

It is proposed that the new law: (1) prescribes strong, swift and scalable **remedies against over-removal of legitimate content**, including through an external ADR (that would be financed by higher fees paid by providers which erroneously take down the content and lower fees by users who complain without success) to **incentivise better internal quality review**; (2) sets concrete incentives for high-quality notification and review process by means of elaborate rules developed through technical standardisation in different areas; (3) clarifies the **passivity criterion by linking it to editorial choices** and thereby avoiding discouragement of voluntary preventive measures; (4) includes a set of **new safe harbours**, at least for hyperlinks, search engines and domain name authorities; and (5) creates an EU-wide legal basis for **targeted measures** (preventive or corrective) responding to the risks posed by the hosting providers provided that the evidence suggests a failure the notice and takedown process and that they remain compliant with the no monitoring obligation and fundamental rights.

Since the adoption of the ECD in 2000, many EU legislations and enforcement tools and institutions relating to the provision of Information Society Services have been adopted (some are more general and covering all services provided in the EU internal market while others are more specific and cover only specific categories of Information Society Service). It is essential that **the puzzle rules applicable to online platforms and their enforcement mechanisms are coherent and effective**. ECD should be made consistent with those new general rules, in particular by streamlining transparency and information requirements. Also the regulation of the different types of Information Society could be more coherent, in particular by improving the baseline liability regime of online platforms (as explained above) and by strengthening the regulation of online advertising. For those two issues, the new rules imposed by the **Audio-visual Media Services Directive (AVMSD)** on the video-sharing platforms are a **good starting point**.

Smart regulatory techniques such as **self- and co-regulation should continue to be encouraged** given the rapid and uncertain market evolution as well as the exponential increase of online content. However, to respect our EU values, in particular our human rights and rule of law, **better safeguards need to be set up**. In particular, Codes of conduct should be accepted by the main stakeholders representing all the interested parties and values and that their implementation should be regularly monitored in a transparent and independent manner.

The revision of the ECD which is the horizontal and applicable to all the providers of Information Society Services in Europe could be accompanied by **two complementary reforms** within the Digital Services Act to take technology and market developments into account.

- The first complementary reform could **increase the incentives for data sharing and mobility**. Given that sectors differ widely, it would be advisable to use experimental regulatory techniques (such as regulatory sandbox), legislation with sunset clauses and time-limited incentive-based schemes. Moreover, a distinction between personal and non-personal data should be avoided. Any data sharing should actively engage with data protection framework, even if the exposure to its might be only marginal in practice.

- The second complementary reform could consist in the adoption of **stricter rules for the online platforms raising systemic risks** to the European economy and society. Such asymmetric rules could deal with market power issues that cannot be effectively dealt with by pure ex post competition law and ensure that the markets remain fair and contestable. They could also deal with the diffusion of online illegal and harmful content. Those asymmetric rules **could be enforced by an EU regulator** to ensure effectiveness and internalise the cross-countries externalities but **in close partnership with the national regulatory authorities** to meet the principle of subsidiarity. In that regard, the enforcement of financial regulation on the systemic banks by Single Supervisory Mechanism within the ECB is an interesting starting point. At the very minimum, the coordination between national regulatory authorities and the division of work between them should be improved and ensure an effective law enforcement.

4.1. Our assessment of the Directive

4.1.1. The concept of Information Society Service and the regulation of the collaborative economy

The **concept of Information Society Service**, to which the ECD refers to determine its scope, is based on four conditions (*i.e.* service, provided at distance, by electronic means, at individual request) that proved to be **robust over time and applicable to new business models** such as in the sharing economy. Indeed, in its recent case-law, the Court of Justice decided that if a collaborative economy platform does not exercise a decisive influence on the existence and the conditions of the underlying service intermediated by the platform, the platform does offer an ISS. This is the case of Airbnb for instance. Conversely, if a collaborative platform does exercise a decisive influence on the provision of the underlying service, the platform does not offer an ISS. This is the case of Uber for instance.

In any case, the ISS qualification and the no prior authorisation principle that derives from it **do not impede on the ability of Member States to regulate the services which are intermediated by the online platform**. In the case of Uber, that is obvious as the online intermediation has been considered as accessory to – and absorbed in - the transport service which can be regulated by the Member States. In the case of Airbnb, the online intermediation service provided by Airbnb is separated from the underlying hosting service and benefits from the no prior authorisation rule. However, the hosting service intermediated by Airbnb is not an ISS and can thus be regulated by the Member States. Thus, the concerns raised by some that the no prior authorisation rule severely limits the competence of the Member States to regulate the underlying services intermediated by collaborative economy platforms seem to be unfounded.

The concept of **ISS is also very broad** and, with the progressive digitisation of our economy and society, covers an increasingly important part of the services provided in the EU Internal Market. Given the increasing importance of those services, the baseline regulation contained in the ECD has been supplemented with additional obligations for some categories of ISS contained in specific EU legislations, such as the NIS Directive, the EECC, the P2B Regulation or the new DSM Copyright Directive (see Section 2.3). In some cases, those supplementary obligations may be in tension with the ECD, and **coherence in the interpretation and the application of the different rules applicable to the same category of ISS** is of paramount importance.

4.1.2. Application to non-EU providers

The ECD applies to providers that are established in a Member State by referring to a **classical definition of establishment**: a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider.[167] In recent years, there has been tensions at Member State and EU level linked to the fact that some non-EU tech companies are providing services to EU citizens without necessarily abiding by EU (and national) rules.

Some of the **more recently adopted EU legal instruments take other criteria into consideration to trigger the application of EU rules**. This signals that the traditional criteria of establishment may be no longer adequate.

[167] ECD, recital 19.

- The *GDPR* applies to companies not established in the EU that offer goods or services to individuals in the EU or that monitor their behaviour.[168] Companies not established in the EU but subject to the GDPR have to designate a representative in the EU, unless they process personal data occasionally and without a risk for individuals;[169]
- The *AVMSD* provides that non-EU Video-Sharing Platforms are deemed to be established in a Member State if it has a parent or subsidiary undertaking that is established in that Member State or it is part of a group where an undertaking is established in that Member State. It then goes on to settle how to determine which Member State has jurisdiction in case multiple Member States could claim jurisdiction;[170]
- The *Platform-to-Business Regulation* applies to online intermediation services and search engines, irrespective of their place of establishment, if their services are provided to business users that are established in the EU and that offer goods/services to consumers in the EU.[171]

Moreover, unlike more recent initiatives, also, the ECD does not cover how Member States should **settle how to solve multiple claims to jurisdiction within the EU.**

4.1.3. Internal Market rules: country of origin and harmonisation of user protection

As already stated, the **Internal Market Clause is one of the greatest successes of the e-commerce Directive** as it is the cornerstone of the Digital Single Market. However to be effective, such Internal Market Clause needs to be accompanied by confidence of the Member States (and their citizens) that the regulation in the country of establishment is sufficiently protective and effectively enforced. Such confidence requires, on the one hand, a harmonisation of the main rules aimed to protect users and, on the other hand, cooperation and mutual assistance between the competent authorities of the Member States in charge of enforcing the rules.

Fortunately over time since the adoption of the ECD, both have increased. On the one hand, the harmonisation of protection rules has substantially increased with the strengthening of the B2C consumer acquis (both at the substantive and institutional levels) and the recent adoption of B2B protection rules (thanks to the new P2B Regulation). On the other hand, the tools for Member States cooperation have also be strengthened with the establishment of the e-commerce expert group, the creation and then the reinforcement of the Consumer Protection Cooperation (CPC) Network and the increasing use of the Internal Market Information (IMI) System.

However, improvements are still possible, in particular with regard to **the conditions under which the derogation can be used by the destination Member State to regulate an ISS provider established in another Member State**. The substantive conditions, which are described in Art. 3(4a) of the ECD, could be made more limited as it is done in the AVMSD.[172] In particular, the derogation could be limited to public security, public health or public security. They could no longer be based on consumer protection given the substantial strengthening of the EU consumer acquis since the enactment of the ECD. The procedural conditions, which are described in Art. 3(4b) of the ECD, could set some time limits and improve openness and transparency as it is done by the *Transparency Directive*.[173]

---

[168] GDPR, Art.3 and European Data Protection Board Guidelines 3/2018 of 12 November 2019 on the territorial scope of the GDPR.
[169] GDPR, Art.27.
[170] AVMSD, Art.28(a).
[171] P2B Regulation, Art.1(2).
[172] AVMDS, Art.3(2).
[173] Directive 2015/1535, arts. 5 and 6. Interestingly, in Case C-390/18 *Airbnb Ireland*, the Court of Justice already draws a parallel between the derogation procedure of the ECD and the procedures of the Transparency and decides to impose the same sanction (unenforceability against individuals) when a Member State fails the procedural conditions, in particular a failure to notify to the Commission the national derogatory measures.

Another possible area of improvement could be to **further clarify the notion of 'coordinated field'** which frames the areas covered by the country of origin principle. Although it is defined specifically, it covers potentially very wide areas, which are not altogether harmonised in the Directive: requirements with which the service provider needs to comply for the taking up of the activity of an ISS, such as requirements concerning qualifications, authorisation or notification, the pursuit of the activity of an ISS, 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.

The **eight exceptions to the Internal Market Clause**, contained in the Annex of the ECD, **could also be reviewed to assess whether they are still justified in light of the EU harmonisation** of national legislation that has taken place since the adoption of the Directive. This is particularly true for consumer protection rules, which means that the exception relating to contractual obligations related to consumer contracts may no longer be justified.

Next generation rules should also strive **to put an end to national initiatives which target online platforms** which are ISS which threaten and undermine the Internal Market Clause of the ECD. Some of these national legislations target large platforms which have more than a given threshold of users in the country by inter alia requiring that they appoint a legal representative. These national initiatives are most probably triggered because there is a lack of minimum substantive rules governing the conduct of ISS in the ECD itself. As pointed out above, the conducts of ISS are covered in the more recent sector specific laws such as AVMSD but the scope of application of these initiatives is limited to some specific categories of ISS (such as the video-sharing platforms in the case of the AVMSD).

4.1.4. Liability rules

The criticism of the Directive's liability rules can be grouped as follows: (1) the Directive lacks sufficient safeguards to prevent violations of fundamental rights, in particular freedom of expression; (2) the Directive does not envisage that notifications may be sent by robots and fails to incentivise the quality of sent and reviewed notifications; (3) the Directive does not prevent fragmentation due to diverging application of the passivity criterion by the national courts; (4) the Directive fails to cover hyperlinking and search engines and other new services; (5) the Directive only serves as a limit and not as a comprehensive tool of removal of illegal content.

(1) The **Directive lacks any safeguards to prevent violations of fundamental rights**, in particular freedom of expression. The ECD does not include provisions, which would provide for effective and tested mechanisms to avoid and/or resolve incorrect removals of content. This lack of safeguards leads to over-notification by notifiers, over-removal by providers and under-assertion of rights by affected users. Empirical evidence confirms the above phenomena.[174] Although some recent sectorial initiatives like AVMSD and DSMD include safeguards, even these are arguably very vague.

The potential measures suggested in the literature include carrots and sticks for all these stakeholders in the enforcement chain. In order to work, they need to be scalable,

- For notifiers, potential measures include fines or processing penalties (e.g. delays or suspension of automated submission possibilities for low-quality notifiers) in case of low-quality notifications, enhanced access for notifiers who have a proven record of notification quality, or.
- For providers and affected users, potential measures include transparency to the public and obligation to explain the decisions to affected users, obligatory human review, internal and

[174] See Section 3.1.2.

external dispute mechanism, judicial remedies against providers, and fines for high numbers over-removals.

On the basis of an empirically tested solution, Fiala and Husovec (2018) propose to create the option of an external Alternative Dispute Resolution (ADR), which would be financed by higher fees paid by providers which erroneously take down the content and lower fees by users who complain without success. Such fees are meant to incentivise providers to improve their internal processes and provide a credible remedy to users to get their content reinstated and be heard by an impartial body. The ECD can introduce such option in exchange for taking away legal risks after providers implement ADR decisions. Providers would benefit from legal immunity if they implement the ADR decides. In the laboratory experiments, the solution mitigates the over-removal and increases legitimate complaints by users. An important implementation requirement would be, however, that providers would have to be bound by these ADR decisions at least for some limited time in order to prevent circumvention through changes of terms of service. Otherwise, there is risk that each ADR decision can be instantly circumvented by providers through a simple change in terms of the service. Since the value of user's content usually goes down with passing time, introducing delay to such changes should be sufficient for users to protect their speech interests, while assuring that providers control the 'house rules'.

In addition to safeguards to the removal process, especially in the area of freedom of expression (unlike competition or data protection law), there are no authorities specifically available to resolve or investigate harms associated with platforms. This is especially problematic for the providers whose operations have large impact on people because they set rules which effectively limit social interactions and what people can read or share.[175] These providers are in a special position of power in the public sphere, and should be subject to equally special responsibility to at least explain how they try to protect human rights in designing and operating their services. To enforce such obligation, existing national authorities, such for instance the media regulatory authorities[176] or the ombudsperson (or its equivalent versions) could equipped with investigative powers and reporting duties.

(2) The **Directive does not envisage that notifications may be sent by robots**, not humans, and fails to incentivise the quality of sent and reviewed notifications. This criticism is connected with the previous one. Empirical studies document that automation of notifications is responsible for their rise. ECD assumed that notifications are sent by humans, which is clearly outdated. Moreover, we see a rise of outsourcing of notification activity to professional service providers, like law firms or enforcement agencies. The ECD should recognise the role of these parties, and of the technology they use, and set the right incentives for them to generate and send only high-quality notifications (e.g. through a certification procedure based on the sectorial standardisation); otherwise, they could face sanctions such as fines, suspension of access to automated submission of notifications, a decrease of public funding (for state-funded NGOs), or similar consequences.

(3) The **ECD does not prevent fragmentation due to diverging application of the passivity criterion by the national courts**. The stakeholders obviously disagree about the correct scope of passive/active criterion. It is undeniable, however, that the passivity criterion is responsible for some divergence in the case-law concerning the hosting safe harbour[177] and that it discourages rather than encourages more preventive measures. The criterion is a reason why some of the national courts avoid application of the ECD framework (as active services are out of the scope).

[175] As argued in a companion Study: Enforcement and cooperation between Member States, Smith, M (2020).
[176] AVMSD, Art.30. The media regulator and their cooperation at the EU level have be strengthened by the revision of the AMVSD in 2018.
[177] van Hoboken et al. (2018) p. 36.

To facilitate harmonization, several authors suggest to either abandon the criterion for hosting or to clarify it.[178] Same demands surface in the 2016 Commission consultation. The main policy concern behind the passivity criterion is that it potentially *discourages* voluntary preventive measures by the providers (at least in some Member States),[179] who might be afraid to lose their safe harbours if they take those preventive measures (so called 'good Samaritan paradox'). This is obviously counter-productive, because the ECD in essence aims to incentivise more preventive actions to be taken by providers. If a lack of clarity about the issue too easily cancels outs the reassurances of the hosting safe harbour, the ECD fails to achieve its intended effects – to effectively remove illegal content. Similarly like AVMSD, some proposals therefore suggest that the core of the distinction should be about editorial choices made (as they appear to the consumers).[180] If a piece of content is adopted by the provider as their own editorial content, they should not benefit from provisions which are covering only its non-editorial counter-part provided by third parties. Since this will be complemented by a system of accountability, the internal differentiation of preventive measures will take place anyway, but it will be based on the assessment of the risk posed by each type of hosting provider based on evidence (see below).

(4) The **Directive failed to include hyperlinking and search engines; it does not cover also other new services**. As a consequence, it has been criticised for missing out on socially valuable services.[181] Other examples of services which are not covered include domain name authorities, domain registrars, online payment services and autocomplete or autosuggestion services. Some of these services were rarely targets of litigation, others were more often. It might be worth considering an extension of safe harbours to cover these other services, as that could establish clarity about the models of enforcement against these players. Because the services generally differ by their proximity to user's behaviour, on the scale of involvement between hosting and mere conduit services, potential new safe harbours could operationalize these two provisions as models of enforcement for different services.

(5) The **Directive only serves as a limit and not as a comprehensive tool of removal of illegal content**. Because the Directive only provides for a broad framework, the Member States can establish different rules under its umbrella,

- First, the Directive creates a legal basis neither for reactive removal (as it does not ever establish liability), nor for specific duties (e.g. to terminate accounts for repeated illegal uploads). The Member States might foresee different notice and takedown processes for hosting services. This creates a challenge for the Digital Single Market as notifications, removals and complaints cannot be simply scaled across the EU. They can have different systems of specific preventive or corrective duties;
- Second, the importance of the EU framework might differ across the Member States given that the consequences following the loss of a safe harbour can be of a different magnitude. For instance, losing a hosting safe harbours in one country could immediately lead to liability, while in others, any liability might require further conditions to be met. This complicates the private and public enforcement;
- Third, the lack of specificity of the Directive allows bad actors to escape good practices when implementing the notice and takedown system.

[178] Rosati (2016); Angelopoulos (2016); Stalla-Bourdillon (2016); Husovec (2017a), p. 56-57 (for reformulate).
[179] See Part 2.4.
[180] Husovec (2017a), p. 56-57.
[181] See van Hoboken (2009).

> Two countries thus can have very different experiences with the same type of policy because they regulated the process of knowledge acquisition and the subsequent response differently. To address these challenges, some commentators propose more detailed rules, in line with the Commission Recommendations, which would define the process on the EU level.[182]

Husovec (2018; 2020) suggests to legislate only on the essential requirements of the process, and then leave the details to the standardisation process at the European Standards Organizations (CEN, CENELEC and ETSI), which can better reflect industry-wide "best practices" in different areas. Following the New Approach, such technical standards could then serve as a proof of the provider's "best efforts" to comply with the notice and takedown system as diligently as possible. Technical standardisation could, unlike existing frameworks, better foresee and keep up with automation, new techniques used and other market developments. It would be also more formalised, evidence-based and technically-oriented than the DSM Copyright Directive's Stakeholder Dialogues.[183] This approach also allows more flexible definition of the needs of SMEs, as it does not set fixed criteria in stone through legislation.[184]

In the same spirit, the legislator could address the lack of legal basis for *specific preventive or corrective measures* in the context of hosting services, which are only tolerated and not specifically regulated by the ECD. These measures are easier to harmonise than liability following the loss of the safe harbour.[185] In order to avoid sidestepping the existing ECD framework, the possibility would be to expect "best efforts" implementation of the notice and takedown system as a baseline to avoid any liability for third party content for the hosting providers. Only if such system demonstrably fails, a procedure could be envisaged to unlock an EU-wide legal basis imposing additional specific preventive or corrective measures, which would be dealt with by the courts, under the coordination of the Court of Justice jurisprudence. Such responsibility for specific preventive or corrective duties could be also separated from the underlying liability for content and potentially take other regulatory forms. In any case, it is important that the inquiry shifts into risk management rather than the circumstances of individual incidents, which are little informative for overall "best efforts". The advantage of this approach is that it avoids the problem of coordination of liability establishing rules, which would have to cover too many areas. The legislator can use the rules in the area of IP law[186] for inspiration, however, with some adjustments. Firstly, the regulatory authority should be primarily vested in an administrative authority under the guidance of the courts, as many areas of illegal content would not be litigated directly before the courts because plaintiffs might be lacking. Second, such authorities should base their actions more on the market evidence of failures. They should assess of the risk posed by the platforms and how to mitigate it. Such system also allows to internally differentiate between different types of hosting providers active in different areas.

4.1.5. Smart regulatory mechanisms

The ECD encouraged the reliance on alternative and smart enforcement tools, in particular the use of self- and co- regulation to establish the rules and of out-of-court dispute settlement to contribute to a better enforcement of the rules.

---

182 Kuczerawy (2018); de Streel, Buiten, Peitz (2018).
183 See https://ec.europa.eu/digital-single-market/en/stakeholder-dialogue-application-Art.-17-directive-copyright-digital-single-market
184 Compare with Art. 2(6) of the DSM Copyright Directive.
185 Which faces a problem of too many legal areas and types of liability.
186 See Art. 8(3) of the Information Society Directive (Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society) and Art. 11 third sentence of the IP Enforcement Directive – for more see Husovec (2017a).

The **use of self- and co-regulation** tools may be justified when technology and market evolve quickly and the asymmetry of information between the stakeholders and the authorities is high. In this case, it may be difficult, if not impossible, for the legislator to impose the appropriate obligations and remedies. Indeed, we have seen that Code of conducts were very much encouraged by the Commission to limit the spread of harmful or illegal content and material online. However, there is an obvious risk that self-regulation is self-serving[187] and/or is not well enforced. Therefore, Codes of conduct should comply with the principles for better self- and co-regulation proposed by the Commission.[188] As explained above, those principles ensure that rules are prepared openly and by as many as possible relevant actors representing different interests and values, are monitored in a way that is sufficiently open and autonomous and are sanctioned when violated.[189]

Although the European Commission publishes evaluations reports concerning several Codes of Conducts on tackling illegal or harmful content, due to lack of transparency around the underlying methodology (in particular concerning the notification practices of NGOs, what is considered to be their legal benchmark, their internal quality review, and the sampling of their notifications), the presented numbers have limited value. [190] In other words, without further data, the reports cannot be taken as presenting "objective compliance rate" or other phenomena as the exercise might not be representative enough or instead be observing disagreement about the basic operation of the system (e.g. which rules to consider).

The **use of alternative dispute resolution**, in particular online, may also be justified when disputes are many and could be easily solved, possibly with the help of automated tools. Indeed, as explained above, there is an increasing automation in the detection and the removal of illegal content online. However, it is important that fundamental rights, in particular due process, are respected and that the last word on possible balance between fundamental rights is left to the courts of the Member States and the EU.

4.1.6. Adaptation to technological and market changes

The **increased concentration of digital markets** has prompted debates about further intervention through regulation. These interventions can be motivated by competition concerns – namely, the problem of market tipping – or innovation concerns – namely, under-use of existing innovation inputs (e.g. data).[191] This may justify additional and **stricter rules as well as distinct and more EU-based enforcement mechanism for the biggest platforms** which pose systemic risks for the European economy and society. Some recent legislations already differentiate obligations according to the size of the platform, applying explicitly or implicitly a proportionality principle and/or risk-based approach.[192]

---

187 As argued in a companion Study: Enforcement and cooperation between Member States, Smith, M, (2020). Also Bartle and Vass (2007).

188 Those principles are available at: https://ec.europa.eu/digital-single-market/en/best-practice-principles-better-self-and-co-regulation.

189 See also, Finck (2018).

190 European Commission, Code of Conduct on countering illegal hate speech online: fourth evaluation confirms self-regulation works, Factsheet, February 2019, available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#theeucodeofconduct (the fourth evaluation of January 2019 showed that 88.9% of notifications were reviewed within 24 hours (as opposed to 40% when the Code of Conduct was adopted in 2016) with a removal of 71.7% on average of the reported illegal hate speech).

191 Crémer, de Montjoye and Schweitzer (2019); Drexl (2018).

192 AVMSD, Art.28b(3); DSMD, Art.17(6).

As already noted by the Commission, such additional rules could, among others, 'ensure that markets characterised by large platforms with significant network effects acting as gatekeepers, remain fair and contestable for innovators, businesses, and new market entrants'.[193]

The most discussed regulatory intervention is **data sharing**, which is presented as a possible ex-ante regulatory measure, which could potentially address both competition and innovation concerns.[194] Obviously, two rationales suggest different designs of possible interventions, and therefore should be distinguished in practice. While the former one is inextricably linked with the market power, the latter is not. Moreover, as pointed out in the literature, there are different types of data access policies, which range from one-off data portability to real-time data access, from freely-licensed to free-based sharing and from B2C to B2B regimes.[195]

In the last few years, the EU has instituted a number of data related policies, which include some type of data-sharing element.[196] The OECD (2019) noted that data access and sharing is estimated to generate social and economic benefits worth between 0.1% and 1.5% GDP in the case of public-sector data, and between 1% and 2.5% of GDP (in a few studies up to 4% of GDP) when also including private-sector data. Our report is too limited to engage in a detailed debate, however, it can point out some high-level principles for possible data-sharing obligations, which might be considered in Digital Services Act.[197]

Firstly, some new initiatives are increasingly making **a distinction between personal and non-personal** data. This has been criticised as perhaps have some rationale in case of data localization requirements, but as **very problematic as a starting point for new innovation policy**.[198] Data protection considerations should always stay at the heart of data sharing schemes. Even though some data sets might pose lower risks, as they do not regularly involve personal data, this can easily change. Therefore, new data sharing policies should not be predicated on unworkable and unsustainable notions of non-personal data. They should try to design data protection and innovation rationales into same regulatory fabric. This means that any data sharing should actively engage with data protection framework, even if the exposure to it might be only marginal in practice.

Secondly, given that **data-sharing needs and practices might differ across the sectors**, it might be advisable to use experimental regulatory techniques, such as legislation with sunset clauses, time-limited incentive-based schemes (e.g. tax-discounts, subsidies, regulatory concessions) in order to facilitate data sharing. Such tools can be evaluated, redesigned, compared and then improved upon. Since interventions are likely to be needed in specific sectors and areas, it would be advisable to keep the solutions flexible enough.[199]

4.2. Recommendations for improvement

On the basis of our assessment of the e-commerce Directive, this last Section proposes some improvements. The recommendations are presented by order of priorities for the reform of the ECD. Then, there is one recommendation which is not currently included in the ECD, but could made part of the future Digital Service Act.

---

193 Communication from the Commission of 19 February 2020, Shaping Europe's digital future, COM(2020) 67, p.10.
194 Communication from the Commission of 19 February 2020, A European strategy for data, COM(2020) 66 and Commission Staff Working Document of 25 April 2018, Guidance on sharing private sector data in the European data economy, SWD(2018) 125. See also: Alexiadis and de Streel (2020).
195 For overview, Graef, Husovec, van den Boom (2019).
196 Graef, Husovec, van den Boom (2019); Graef, Tombal and de Streel (2019).
197 Communication from the Commission of 19 February 2020, A European strategy for data, COM(2020) 66.
198 For broader criticism, see Graef, Gellert, and Husovec (2019).
199 Flexibility and experimentation are also suggested by Ctrl-Shift (2018).

4.2.1. Priority 1: Maintaining the Internal Market Clause to alleviate the fragmentation of the Internal Market

As the **Internal Market Clause** (Art. 3(2) ECD) is the cornerstone of the Digital Single Market, the clause should absolutely be maintained and should not be undermined by any revision of the ECD. However, the system for derogation to the clause could be improved. The substantive conditions (in art. 3(4a) ECD) could be limited to public policy, health and security reasons[200] and the procedural conditions (in art. 3(4b) ECD) could include time limits and more transparency.[201]

At the same time, the **cooperation and mutual assistance between Member States**, in particular between the country of origin where the provider of ISS is established and the country of destination where the provider is offering its services, should be strengthened by providing specific procedures and deadlines. In particular, the ECD could integrate the cooperation mechanisms that have been developed since 2000, such as the e-commerce expert group, the Consumer Protection Cooperation Network and the use of Internal Market Information (IMI) System.

Moreover, a **separate and more EU-based enforcement mechanism** could be foreseen for the systemic platforms when the ability and/or the incentives of the authorities of the Member State where the platform is established are insufficient to guarantee an effective law enforcement (see below on the complementary priorities).

The ECD, and its Internal Market Clause, could also cover the **online platforms which are not established in the EU** but provide their services to EU customers. To do that, the ECD could follow the systems adopted in more recent EU legislations such as imposing the designation of a representative in the EU (as done with the GDPR). The ECD could also cover how Member States should **settle how to solve multiple claims to jurisdiction within the EU** (as done with the AVMSD) and envisage including a transparent register listing the Member States having jurisdiction over a given ISS provider, which could be maintained by the European Commission.

4.2.2. Priority 2: Improving liability rules to ensure a safer Internet

Given its success, the **liability safe harbours** for the digital platforms currently covered by the ECD (art 12-14: mere conduit, caching and hosting) should be preserved.

To improve the efficiency of the rules, a complete framework for a **Notice-and-Takedown process** with detailed provisions on exchange of notifications and their evaluation should be included in the ECD along the following lines,

- The framework should reflect the reality that a majority of notifications today are sent by robots, not humans;
- It should provide incentives for low error rates in notifications and their processing, for instance with fines, suspension of submission, or fees-attached Alternative Dispute Resolution (see below);
- Following the New Approach adopted by the EU in the eighties for the harmonisation of rules regarding goods, the Notice-and-Takedown rules could define the essential requirements for the process, and leave the technical details to the European Standards Organizations (CEN, CENELEC and ETSI).

[200] See AVMDS, Art.3(2).
[201] As in Directive 2015/1535, arts. 5 and 6.

It should also be clarified that the **only interventions which amount to adoption of the third-party content as one's own** (as judged by average consumers) should **lead to a loss of a safe harbour** due to their active nature. In line with AVMSD, this would shift the enquiry into editorial and non-editorial roles. Being helpful should not come at the cost of exposing oneself to liability risks for non-editorial choices (thus addressing the 'good Samaritan paradox'). At the moment, the notion of active nature of the services discourages providers from taking more action, as the more preventive they become, the likelier they are to fall outside of the safe harbour. Adopting objective test – how an average consumer judges the editorial role – could facilitate clarification of the requirement.

In addition, a **new regime for other services** which are currently not covered by any of the safe harbours, at least for search engines, hyperlinking and domain name authorities, should be created, drawing on models for hosting and mere conduits services. The prohibition of general monitoring should equally apply to these services.

Since Notice-and-Takedown might fail in practice for some services, in order to create a future proof framework, it might be advisable to include a possibility to **impose further obligations of targeted best efforts imposing specific preventive and corrective duties for the hosting providers which are proportionate to the risks generated by the service**,

- This possibility should be subject to strong evidence that diligent notice and takedown fails for a particular class of services. Factual evidence should be for instance reviewed by a single EU-wide independent body, like Regulatory Scrutiny Board, and endorsed by an implementing decision of the Commission;
- Upon such acknowledgement, for some services, national independent competent authorities[202] (which are subject to judicial review) may then be allowed to impose targeted best efforts measures (compliant with no monitoring obligation) provided that effects on fundamental rights are not negative;
- The Court of Justice of the EU would assure harmonization of such measures and their observance of fundamental rights.

This additional responsibility to implement such measures would be independent from liability for third party content. Such accountability mechanism would supplement lack of existing rules establishing liability in similar way as the injunctions against intermediaries do in the context of intellectual property rights.[203]

Very importantly, **fundamental rights should be protected more effectively** by introducing a number of safeguards against frequent over-removal of legitimate content,

- First, expansive rules on **transparency concerning content removals**, their processing, mistakes, actors and notifications could be introduced with personalized explanations for affected users and audits for authorities or researchers;[204]
- Second, a possibility of **external Alternative Dispute Resolution bodies (ADR), which would resolve complaints of affected users at the expense of providers** (in case they made a mistake) could be introduced.

[202] This possibility is already acknowledged by Art. 12-14 ECD.
[203] Nordemann (2020) also suggests to expand the legal mechanism used for accountability for injunctions in the area of IP rights.
[204] As recommended by the High-Level Expert Group on Artificial Intelligence (2019) and by the European Parliament Resolution of 12 February 2020 on Automated decision-making processes: Ensuring consumer protection, and free movement of goods and services.

Providers would benefit from legal immunity if they implement ADR decisions. Such ADR system will not only give credible remedy to users, and thus improve the complaint rates, but also incentivise higher quality of internal complaint mechanisms by providers (as these avoid ADR-related costs). However, effective ADR and any other dispute resolution require that providers distinguish violations of law from those of Terms of Services. An important implementation requirement therefore should be that providers would have to be bound by these ADR decisions at least for some limited time. Otherwise, there is risk that each ADR decision can be instantly circumvented by providers through a simple change in terms of the service. Since the value of user's content usually goes down with passing time, introducing delay to such changes should be sufficient for users to protect their speech interests, while assuring that providers control the 'house rules'. If the external ADR works well, it incentivises for good internal quality control of notifications in the long run (e.g. using internal ADR, human review, etc.).

Finally, the **providers whose operations have large impact** on people, such as their right to freedom of expression, should have **a special responsibility** to explain how they try to protect human rights in designing and operating their services. This obligation to explain may correlate with the competence of a national authority, such as the media regulator or the ombudspersons to process individual's complaints and request specific information, including of confidential nature. Those authorities could then collaborate and coordinate through an EU-wide network.

4.2.3. Priority 3: Ensuring coherence among EU rules to alleviate the fragmentation of EU regulatory framework for Information Society Services

One the main principles of the *Commission Better Regulation Guidelines* is the **coherence within each EU law and among EU laws and policies**.[205] Given that the ECD covers a wide range of services which are also covered by other general or specific EU legislations, it is key to ensure the coherence of the ECD with those other rules.

Coherence should be ensured **with the general legislations** which apply to the provision of all services in the EU. In particular, the different **information to be provided** to the users of digital platforms (currently spread between Art. 5 for information regarding the platforms and Art. 10 for information regarding the electronic contract) could be grouped together and streamlined with the information disclosure requirements imposed by more recent EU law, in particular the Consumer Rights Directive and the Platform to Business Regulation.[206]

Moreover, such information should be **transmitted to the users in an effective manner taking into account the numerous biases and heuristics** of humans shown by the recent behavioural studies. In particular, the quantity of the information should be limited to the most relevant one and presented in an attractive manner[207] and at the right moment when the user should take the decision.

Coherence should also be ensured **with the specific legislations which apply to the provision of particular categories of ISS** (such as intermediation or search platforms, interpersonal communications platforms, video sharing platforms or online content sharing platforms).

---

[205] Commission Staff Working Document of 7 July 2017, Better Regulation Guidelines, SWD(2017)350, pp.62-63.

[206] Directive 2011/83 on consumer rights, as amended by Directive 2019/2161 and Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services.

[207] The recent research on legal design is also useful in that regard: https://www.legaldesignalliance.org/.

As we have seen, coherence is particularly needed for the **liability regime** in case of illegal online content. It is also needed for the regulation of **commercial communications** on online platforms.

Art. 7 of the ECD could therefore be strengthened as it was done for video sharing platforms in the revised AVMSD, in particular, by specifying in more details the transparency and qualitative requirements.[208] Moreover, the effects of the imposition of ad capping on some online platforms as it is already the case for traditional broadcasting could be further examined.[209]

4.2.4. Priority 4: Continuing to rely on smart regulatory techniques to ensure effective implementation

Code of Conducts (art. 16 ECD) should continue to be encouraged as they can be very useful in fast moving industries where the best manners to achieve regulatory goals set in the law are not easy to determine. However, given their increasing importance, the ECD should impose **additional safeguards** on the manner such Codes are established and monitored in order to increase their legitimacy, their effectiveness and compliance with fundamental rights. In particular, the ECD could impose, on the one hand, that the Code of conduct should be accepted by the main stakeholders representing different interests and, on the other hand, that their implementation should be regularly monitored independently and in manner which is transparent and with clear methodologies.[210]

The **out-of-court dispute settlement** (art.17 ECD) should be **aligned with more recent EU law** adopted in the consumer field, in particular the Alternative Dispute Resolution for consumer disputes Directive[211] and Online Dispute Resolution for consumer disputes Regulation.[212] Moreover, as explained above, external Alternative Dispute Resolution bodies could be foreseen in the context of the new rules on Notice-and-Takedown to contribute to the protection of fundamental rights.

4.2.5. Complementary priorities within the Digital Services Act

Besides the reform of the existing pillars of the ECD, the new Digital Service Act could include two complementary reforms. First, the incentives for data **exchange and sharing** should be increased given the importance personal and non-personal data have taken with the development of big data and Artificial Intelligence techniques. Those incentives should relate to personal and non-personal data at the same time, a distinction which is increasingly difficult to draw and less and less sustainable.

Given that data-sharing needs and practices might differ across the sectors, it might be advisable to use experimental regulatory techniques, such as legislation with sunset clauses, time-limited incentive-based schemes (e.g. tax-discounts, subsidies, regulatory concessions) in order to facilitate data sharing. Such tools can be evaluated, redesigned, compared and then improved upon. Since interventions are likely to be needed in specific sectors and areas, it would be advisable to keep the solutions flexible enough, and avoid sweeping rigid horizontal instruments.

Second, **stricter rules for the online platforms raising systemic risks** for the European economy and society may be adopted. Those rules should ensure that the important opportunities brought by the biggest online platforms are seized while the risks are mitigated. They should also recognise the variety of business models among online platforms.

---

208 AVMSD, Art.28b(2).

209 AVMSD, Art.9-11 for transparency requirements and Art.23 for ad capping. See Newman (2019, p. 39) suggesting rules that would limit Internet advertisements to a certain maximum portion of a given page, a restriction on the number and/or size of pop-up advertisements allowable on a given page.

210 See AVMDS, new Art.4a introduced by Directive 2018/1808.

211 Directive 2013/11 on consumer ADR.

212 Regulation 524/2013 on consumer ODR.

Such asymmetric rules may be justified, on the one hand, to tackle some market power issues and ensure that the markets remain fair and contestable and, on the other hand, to tackle of the diffusion of online illegal and harmful content.

Those asymmetric rules **could be enforced by an EU regulator** to ensure effectiveness and internalise the cross-countries externalities but **in close partnership with the national regulatory authorities** to respect the principle of subsidiarity. In that regard, the enforcement of financial regulation on systemic banks by Single Supervisory Mechanism within the ECB is an interesting starting point. [213] The feasibility and the relevance of establishing an EU regulator for those systemic platforms could be explored. At the very minimum, the coordination between national regulatory authorities and the division of work between them should be improved and ensure an effective law enforcement.

[213] EU Financial Supervision Regulation provides for a systemic power analysis based on the following criteria: (i) the size - total value of its assets exceeds €30 billion; (ii) the economic importance for the specific Member State or the EU economy as a whole; (iii) the size of the cross-border activities - the total value of its assets exceeds €5 billion and the ratio of its cross-border assets/liabilities in more than one other participating Member State to its total assets/liabilities is above 20%; or (iv) the direct public financial assistance when the bank has requested or received funding from the European Stability Mechanism or the European Financial Stability Facility. The banks meeting the systemic threshold are regulated at the EU level by the Single Supervisory Mechanism while the other banks continue to be supervised by their national supervisory bodies: Council Regulation 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions, O.J. [2013] L 287/63.

REFERENCES

- Alexiadis P. and A. de Streel (2020), Designing an EU Intervention Standard for Digital Platforms, EUI Working Paper-RSCAS 2020/14
- Angelopolous C. (2016), European Intermediary Liability in Copyright: A Tort-Based Analysis, Information Law Series Volume 39, Kluwer
- Bartle I. and P. Vass (2007), 'Self-regulation within the Regulatory State', 85 Public Administration, 885-905
- Bruegel (2019), Braver, Greener, Fairer, Memos to the EU leadership 2019-2024
- Cappello M. (ed.), Self- and Co-regulation in the new AVMSD, IRIS Special, European Audiovisual Observatory
- Centre on Regulation in Europe (2019), Ambitions for Europe 2024, White Paper
- Christensen M., A Conte, F Di Pietro, P Lecca, G Mandras and S Salotti (2018), The third pillar of the Investment Plan for Europe: an impact assessment using the RHOMOLO model. JRC Working Papers on Territorial Modelling and Analysis 02/2018
- Copenhagen Economics (2007), Economic impact of the electronic commerce Directive, Study for the European Commission
- Crémer, J., de Montjoye, Y.-A. and H. Schweitzer (2019). Competition policy for the digital era, Report to the European Commission
- Ctrl-Shift (2018), Data Mobility: The personal data portability growth opportunity for the UK economy, Report for the UK Department for Digital, Culture, Media & Sport, Available at: https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf
- de Streel A., M. Buiten and M. Peitz (2018), The Liability of Online Platforms: Should exceptionalism end?, CERRE Policy Report
- de Streel A. and C. Hocepied (2019), Contribution to Growth: European Digital Single Market – Delivering improved rights for European citizens and businesses, Study for the IMCO Committee of the European Parliament
- de Streel A., A. Kuczerawy and M. Ledger (2019), 'Online Platforms and Services', in L. Garzaniti et al (eds), Electronic communications, Audiovisual Services and the Internet: EU Competition Law and Regulation, 4th ed., Sweet & Maxwell, 125-157
- Drexl J. (2018), Data access and control in the era of connected devices, Report for BEUC
- Ecorys (2016), An economic analysis of the impact of some online intermediaries on the distribution of copyright protected content, Study for the European Commission
- Smith M., Enforcement and cooperation between Member States, Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020, Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648780/IPOL_STU(2020)648780_EN.pdf

The e-commerce Directive was adopted in 2000 and has played a key role in the development of online platforms in Europe. The study assesses the effects of the Directive as a cornerstone of the Digital Single Market. On that basis, it proposes some reforms for the future Digital Services Act.

This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies at the request of the committee on Internal Market and Consumer Protection (IMCO).

PE 648.797
IP/A/IMCO/2019-07

Print ISBN 978-92-846-6568-6| doi: 10.2861/210544 | QA-01-20-280-EN-C
PDF ISBN 978-92-846-6567-9| doi: 10.2861/609236| QA-01-20-280-EN-N