Liability of online platforms

STUDY

Panel for the Future of Science and Technology

EPRS | European Parliamentary Research Service

Scientific Foresight Unit (STOA)

PE 656.318 – February 2021

EN

Liability of online platforms

Given the central role that online platforms (OPs) play in the digital economy, questions arise about their responsibility in relation to illegal/harmful content or products hosted in the frame of their operation. It is therefore necessary to assess the adequacy and efficiency of the extant EU legal framework, in particular with respect to the liability exceptions provided by the e-Commerce Directive, and to ensure adequate protection for users and their fundamental rights and freedoms (e.g. freedom of expression and of information).

Against this background, the study reviews the main legal/regulatory challenges associated with the operation of OPs and analyses the incentives for OPs, their users and third parties, to detect and remove illegal/harmful and dangerous material, content and/or products. To create a functional classification which can be used for regulatory purposes, it discusses the notion of OPs and attempts to categorise them under multiple criteria. The study then maps and critically assesses the whole range of OP liabilities, taking hard and soft law, self-regulation, as well as national legislation into consideration. To do so, the study distinguishes between liabilities connected with the activities performed or the content uploaded by OP users – from the liability exemptions established by the e-Commerce Directive, to the sectoral rules provided in media law, intellectual property (IP) law, product safety and product liability, protection of minors, hate speech, disinformation and voting manipulation, terrorist activities – and alternative sources of liability, such as OPs' contractual liability towards users, both businesses and consumers, as well as that deriving from infringements of privacy and data protection law.

Finally, the study drafts policy options for an efficient EU liability regime: (i) maintaining the status quo; (ii) awareness-raising and media literacy; (iii) promoting self-regulation; (iv) establishing co-regulation mechanisms and tools; (v) adopting statutory legislation; (vi) modifying OPs' secondary liability by employing two different models – (a) by clarifying the conditions for liability exemptions under e-Commerce Directive, or (b) by establishing a harmonised regime of liability.

AUTHORS

This study was written by Andrea Bertolini, Assistant Professor of Private Law of the Scuola Superiore Sant'Anna (Pisa), and Director of the Jean Monnet Centre of Excellence on the Regulation of Robotics and Artificial Intelligence (EURA), Francesca Episcopo and Nicoleta-Angela Cherciu, Research Fellows in Private Law of the Scuola Superiore Sant'Anna (Pisa), and Junior Fellows of the Jean Monnet Centre of Excellence (EURA), at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

ADMINISTRATOR RESPONSIBLE

Mihalis Kritikos, Scientific Foresight Unit (STOA)

To contact the publisher, please e-mail stoa@ep.europa.eu

LINGUISTIC VERSION

Original: EN

Manuscript completed in February 2021.

PE 656.318
ISBN 978-92-846-7499-2
doi: 10.2861/619924
QA-03-20-811-EN-N

http://www.europarl.europa.eu/stoa (STOA website)
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

1. Introduction

Online platforms (OPs), although not an entirely new phenomenon, have gained significant economic and societal importance in the last decade and the public debate on their responsibilities and liability has reached an unprecedented level. OPs have penetrated all product and service markets and have changed the way in which goods are sold and purchased, and in which information is exchanged and obtained, allowing a shift from the offline world to the online environment, where they provide a myriad of digital services.

Hosting platforms have reached a central role in allowing access to and exchange of information permitting the mass diffusion of any type of content, both legal and illegal. This raised pressing questions on their responsibility in preventing its diffusion, detection and subsequent removal, and platforms' role in the digital realm has morphed, from that of mere hosting providers to that of actors governing how content is displayed and shared online, undertaking certain actions such as moderation, curation and recommendation. Moreover, next to plainly illicit material, other harmful content emerged, potentially affecting the social and political discourse, as well as everyday interactions occurring increasingly online.

This has led to the need to assess the adequacy and efficiency of the extant EU legal framework, in particular with respect to the e-Commerce Directive and the liability exceptions it provides. This, in turn, raised the necessity to understand the correct balance between the need to ensure adequate protection for users, and of their fundamental rights and freedoms (e.g. freedom of expression and of information).

Finally, OPs challenge both consumers and more traditional business models alike. Indeed, the emergence of large OPs or marketplaces, enabling direct interaction between producers and consumers, poses new challenges to product safety, consumer protection and unfair business practices, raising the issue of the adequacy of the extant legal framework, conceived primarily for traditional businesses and retailers, and a less life-pervasive internet in general.

Against this background, after having described the EU policy approach to OPs (Chapter 3), the study: (i) provides a classification of existing platforms; (ii) identifies and assesses the relevant legal framework at the European level, discussing the policy issues that deserve consideration; and (iii) provides a set of policy options, addressing such concerns and discussing the available alternative approaches to tackle them.

2. Online platforms: a functional definition and classification

The term 'online platform' is used in a variety of ways to indicate extremely broad and diversified sets of services and tools (section 4.1). For the purposes of this study, they are defined as entities which: (i) offer 'over the top' digital services to users; (ii) are or can be operated as two- or multi-sided market business models; and (iii) allow the overall facilitation of interaction between the different sides of the market, even when there is no direct interaction among them (section 4.2).

Therefore, to conduct a legal analysis, an effort needs to be made to classify and therefore describe the different kinds of entities that fall under this notion.

Indeed, platforms differ pursuant to (see section 4.3.1): the activities and functions they serve; the actors they involve and the ways in which they interact with them in their operation; their different

sources of revenue and associated business models; the way in which they use and exploit data; and the level of control they exercise on users' activities.

Different combinations of such criteria allow for the identification of the possible policy issues and concerns, with respect to the application of the existing legal framework – comprised of both hard- and soft-law initiatives – deserving discussion and, in some cases at least, even regulatory intervention. The classification proposed in the study is presented in the table below:

OPs' Classification	
Activities	➢ Web-hosting providers ➢ Search engines ➢ Social media, networking and discussion forums ➢ Online media sharing providers ➢ Messaging platforms ➢ Matchmaking and transaction e-commerce platforms (subcategory: collaborative platforms) ➢ Other matchmaking platforms ➢ File storage and sharing providers ➢ Online advertising platforms
Sector of relevance	➢ e-Commerce ➢ Fintech ➢ Transport ➢ Accommodation ➢ Personal services ➢ Advertising ➢ News and media ➢ Electronic communication ➢ Health care
Use of data	➢ Data-enabled OPs ➢ Data-enhanced OPs
Actors	➢ OPs ➢ Users ➢ Advertisers/Targeters ➢ Economically interested third-parties ➢ Collaterally affected third-parties
Sources of revenues	➢ Revenue from the supply side of the market ➢ Revenue from the demand side of the market: subscription fees; users' ad-free use fee; transaction fees ➢ Revenue from the advertisement and third-party side of the market: subscription fees for advertisement placement; pay-per-click fees, pay-per-impression; pay-per-transaction ➢ Other data-generated revenue: selling the data to data brokers; and/or using the data to create new services and products and/or improve existing services, which is also referred to as value-creation
Level of control	➢ Low-level of control ➢ Medium-level of control ➢ High-level of control

3. The European regulatory framework

Through desk research, the study maps the whole range of OP liabilities, taking hard and soft law, self-regulation, as well as national legislation into consideration, whenever relevant. To do so, it distinguishes between liabilities connected with the activities performed or the content uploaded by OP users, and alternative sources of liability, such as OPs' contractual liability against both their business and consumer users, as well as that deriving from infringements of privacy and data protection law. In doing so, it sets forth a conceptual framework by analysing the difference between responsibility and liability, and the different types of liability, distinguishing, on the one hand, between civil, criminal and administrative liability and, on the other hand, between strict, semi-strict or fault-based liability (see section 5.1). The outcome of this research is summarised below:

Source of Liability	Legislative framework	Target	Measures	Soft law relevant initiatives	Self-regulation
Baseline (all types of illegal content)	Directive 2000/31/EC (e-Commerce Directive/ECD)	All (information society service providers)	Liability exemptions (mere conduit, chasing, hosting)	European Parliament resolution of 15 June 2017 on online platforms and the digital single market Communication from the Commission on Tackling Illegal Content online COM(2017) 555 final Commission Recommendation on measures to effectively tackle illegal content online C(2018) 1177 final	/
Media Law	Directive 2010/13/EU concerning the provision of audiovisual media services (Audio-visual Media Service Directive) amended by Directive (EU) 2018/1808	Video-sharing platform services	Procedural accountability	/	/
Online piracy, IP and copyrights infringement	Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market	Online content-sharing providers	Liability exemption if best efforts are employed	/	Memorandum of Understanding on online advertising and intellectual property rights Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet

Source of Liability	Legislative framework	Target	Measures	Soft law relevant initiatives	Self-regulation
	Directive 2004/48/EC on the enforcement of intellectual property rights Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society	Information society services providers	Injunctions/ preliminary measures	/	/
Child Protection	Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography	General (obligation set on Member States, no reference to OPs)	Blocking and removal measures	The European Strategy for a Better Internet for Children Safer Internet Centres and Alliance to better protect minors online	/
	Directive 2010/13/EU concerning the provision of audiovisual media services (Audio-visual Media Service Directive) amended by Directive (EU) 2018/1808	Video-sharing platform services	Procedural accountability	Global Alliance against Child Sexual Abuse and WeProtect Global Alliance	/
Illegal hate speech	Council Framework Decision 2008/913 on combatting certain forms of expressions of racism and xenophobia by means of criminal law	General (obligation set on Member States, no reference to OPs)	/	/	Code of Conduct on Countering Illegal Hate Speech Online (2016)
	Directive 2010/13/EU concerning the provision of audiovisual media services (Audio-visual Media Service Directive) amended by Directive (EU) 2018/1808	Video-sharing platform services	Procedural accountability	/	/

Source of Liability	Legislative framework	Target	Measures	Soft law relevant initiatives	Self-regulation
	The Network Enforcement Act (NetzDG) of 1 October 2017 *Loi n°2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*	Social networks Platform operators and search engines	Procedural accountability	/	/
Disinformation and voting manipulation	The Network Enforcement Act (NetzDG) of 1 October 2017 *Loi n°2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*	Social networks Platform operators	Procedural accountability	Commission Communication on Tackling online disinformation COM/2018/236 final	Code of Practice on Disinformation (2018)
Terrorist content (provocation to commit a terrorist offence)	Directive (EU) 2017/541 on combating terrorism	General (obligation set on Member States, no reference to OPs)	Blocking and removal measures	Commission Recommendation on measures to effectively tackle illegal content online C(2018) 1177 final	EU Internet Forum
	Directive 2010/13/EU concerning the provision of audiovisual media services (Audio-visual Media Service Directive) amended by Directive (EU) 2018/1808	Video-sharing platform services	Procedural accountability	Commission Proposal on a Regulation on preventing the dissemination of terrorist content online	/
Product Liability	Council Directive 85/374/EEC (Product Liability Directive)	Producers, importers, distributors, suppliers	Liability for defective and unsafe products	/	Product Safety Pledge
	Regulation (EU) 2019/1020 on market surveillance and compliance of products	Information society services providers	Notice and action		/
Contractual liability	P2C - general consumer law	Traders	Prohibited practices/blacklists	ELI Model Rules on Online Platforms	/

Source of Liability	Legislative framework	Target	Measures	Soft law relevant initiatives	Self-regulation
	P2B - Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services	Online intermediation services and online search engines	Transparency and procedural accountability	/	/
	C2C - general civil law provisions on contract formation, performance and remedies for breach	/	Contract formation Performance Remedies for breach	/	/
Data Protection	Regulation (EU) 2016/679 (General Data Protection Regulation/GDPR)	Controllers/processors	Rights and obligation for an effective personal data protection as a fundamental right Data protection by design and by default Security	/	/
	Directive 2002/58/EC (ePrivacy Directive)	Electronic communication services/digital mobile networks	Security in the processing of personal data Notification of personal data breaches Confidentiality of communication	Commission Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications	/

Indeed, this framework is comprised of both hard-law rules at both EU and national level, as well as voluntary instruments such as codes of conducts and memoranda of understanding, which representatives of the industry signed, often with the facilitation or oversight of governmental institutions. Moreover, these rules have different – subjective and objective – scopes of application, with some applying transversally to potentially all OPs, and others applying only to specific types of OPs, infringements or activities. Finally, the call for responsibility on OPs varies substantially: it consists of duties which insist on the generalised liability exemption set out in the ECD, obligations to inform and empower users and adopt procedural and technical tools, as well as duties to block, remove and prevent the re-upload of infringing material.

Overall, the system is complex and often underspecified, and it is difficult for the subjects involved to understand exactly when a given obligation applies to them, and what kind of behaviour is required.

This uncertainty may lead to two different, yet equally concerning alternative outcomes. OPs may limit their engagement in fighting online harmful/illegal content, by presenting themselves as 'mere intermediaries' to benefit from the liability exemption under the ECD. In such a perspective, they could limit their efforts to merely adjusting their terms of services and ensuring formal compliance with information duties, and other relevant obligations resting upon them. Alternatively, they might opt for an 'over-compliance' strategy, increasing the quantity, speed and automation of content-removal, without engaging in adequate contextualisation, or without giving space for counter-notices and rectification, resulting in an overall violation of users' fundamental rights and freedoms.

4. Policy options

Against the analysis of OPs' rights, duties and liabilities under the existing EU regulatory framework, the study suggests a set of policy options which could be used to shape the liability of OPs, and especially that relating to the illegal/harmful content or products distributed and/or made available through their infrastructures, such as content that infringes intellectual property rights (IPR), hate speech, terrorist content, content that harms children, counterfeit and unsafe products.

The policy options are assessed against various criteria (cost and benefits; feasibility and effectiveness; sustainability; risks and uncertainties that may impact the policy and its objectives; coherence with EU objectives; ethical, social and regulatory impacts; effect on EU citizens' fundamental rights and freedoms), and presented along a scale of increasing interventionism. However, with the only exception of the first one (amounting to 'no action'), they can be implemented in combination with one another, whenever compatible.

From a methodological standpoint, the study suggests two complementary approaches. Firstly, OPs' liability constitutes **one element** in the broader regulatory efforts towards the creation of a safe and secure digital environment, which cannot be considered in isolation. Indeed, in some cases, other instruments are more suitable for incentivising OPs to adopt an optimal level of content management and moderation, while OPs' civil liability may be used to ensure full and direct compensation of the victims, under a risk management approach (RMA), namely, by holding them strictly and absolutely liable as a single, clear and unquestionable entry point for all litigation, whenever they are in the best position to manage the risks ex-ante and to ensure compensation ex-post. Secondly, OPs' liability should be 'technology-specific', i.e. address narrowly identified problems posed by specific OPs and for specific infringements. Indeed, the suggested approach conceives regulation as an evolving tool, to be modified together with technological advancement through the constant monitoring of emerging solutions and their social, economic and regulatory impact. In particular, this role could be performed by specifically designed bodies, representing the main reference point for proposing regulatory

intervention and for coordination with national authorities and OPs, as well as for cross-fertilisation among different policies and objectives.

4.1. Maintaining the status quo

Under this option, no action at the EU level would be adopted. The regulatory framework would continue to consist of the exemptions set out in the ECD for intermediary liability, complemented in sectoral legislation with specific duties and specific forms of liability, as well as by self-regulatory initiatives. This option would leave many issues that negatively impact OPs' capacity to step up their efforts in the fight against illegal/harmful content online unaddressed and would leave space for national regulation, further exacerbating legal fragmentation and uncertainty in the field. This study therefore suggests that this option should be discarded.

4.2. Awareness-raising and media literacy campaigns

The EU would direct its efforts at ensuring that Member States and OPs adopt measures to strengthen media literacy and empower users, enabling OP users and society at large to actively promote a safe digital environment. Indeed, the spread of online illegal/harmful content involves many subjects, and users of digital services must have the knowledge, sensibility and actual capacity to identify and report it. However, 'empowering tools' often prove sub-optimal: users and members of society have little incentive to control OPs through their choices or behaviour, and imposing extensive requirements of information, awareness-raising and transparency on OPs may, in itself, not be sufficient to make users aware of their rights and duties. Thus, promoting media literacy and user-empowerment should be used not as a primary solution, but rather in synergy with other, more effective policy options.

4.3. Promoting self-regulation

The EU institutions would further promote self-regulatory instruments, where members of the industry adopt voluntary commitments. This would allow a certain degree of cooperation in identifying shared responsibilities and adequate solutions and enhance OPs' responsibility without hampering innovation. However, public sector objectives are not always aligned with those of private companies, so that relying on self-regulation alone may lead to outcomes that do not match those of public regulators. Moreover, limitations in the range of participants, vaguely formulated commitments, absence of clear objectives and measurable progress indicators, as well as the voluntary nature of the agreements and the lack of significant incentives, strongly limit the efficacy of self-regulatory tools in incentivising OPs' proper management of illegal and harmful content, as well as their capacity to protect users' fundamental rights and freedoms. The study therefore suggests that the promotion of industry self-regulation should not constitute the primary solution to the regulation of OP liability, but rather work in synergy with more effective policy options.

4.4. Establishing co-regulation mechanism and tools

The EU institutions and OPs would cooperate to reach optimal regulatory solutions, e.g. by providing governmental involvement, supervision and enforcement of self-regulatory tools, and/or creating regulatory sandboxes enabling firms to test solutions – such as algorithm-based content filters for detecting hate speech – pursuant to plans agreed with and monitored by a competent authority.

These solutions would ensure stronger public oversight over OP practices while enabling flexible and industry-driven regulatory schemes, subject to constant update and adjustment. The adoption of co-regulation is therefore recommended and preferred to the promotion of self-regulatory tools. Ideally, it could be combined with different policy options, such as adoption of statutory legislation.

4.5. Adopting statutory legislation

The EU would define OPs' duties and liabilities through binding regulation, under different models.

(i) Establishing clear and narrowly-tailored primary duties for OPs

The EU institutions could impose a series of tailored and specific duties on OPs to regulate the management of their infrastructure and content-monitoring tools. These duties can be framed as associated with (civil or administrative, seldom criminal) OPs' primary liability. In particular:

- OPs could be obliged to adopt notice-and-take-down procedures, as well as counter-notice mechanisms and instruments for contesting removal, which should ensure procedural fairness for all subjects involved. Common principles and essential requirements could be defined at EU level, while specific technical methods could be outlined in harmonised standards or delegated acts.
- OPs could be subject to reporting obligations and harmonised rules of procedural accountability. Reporting obligations should be specific and concise, and clearly expose the results of follow-up on removal decisions, to ensure that OPs do not engage in over-removal and impose excessive burdens on their users. Content management policies and mechanisms of large OPs could be made subject to public review and advisory oversight.
- OPs that allow trading and supply of goods and services on their infrastructure could be subject to an obligation to verify the identity of the traders and provide such information to users and third parties that have a legitimate interest. Specific cooperation duties between OPs and market authorities could be strengthened.
- While a general obligation to adopt automated filtering and content recognition should be excluded – as it would lead to over-detection and infringements of users' freedoms and fundamental rights – OPs choosing to adopt such tools could be subject to rules on algorithmic transparency, ensuring a 'right to an explanation' and human oversight.
- OPs could be subject to an obligation to ensure transparency on content management, being required to clearly specify what type of content is prohibited and under which sanction, and how review and reputational systems function, in their Terms of Use.
- OPs could be subject to compliance with essential requirements for the functionality of reputational systems, to be set by binding regulation.
- Specific types of OPs could be required to maintain ideologically neutral services, creating algorithms that foster and promote diversity of content.
- OPs could be subject to a positively harmonised form of liability for failure to cooperate in removing the infringing content and/or activity

Clear obligations may provide greater certainty and safety for companies, users, and society, while monetary sanctions for their infringement may be used to feed a no-fault scheme or compensation fund to be administrated by a centralised authority in Europe, to provide compensation under an RMA. Thus, the establishment of clear and narrowly-tailored primary duties for OPs is highly recommended. Ideally, they could be combined with other solutions, such as a review of OPs' secondary liability.

(ii) Modifying OPs' secondary liability

Model A – Clarifying the conditions for liability exemptions under the ECD

The ECD regime would merely be adjusted, adopting the interpretations and practices developed by the European Court of Justice (CJEU) and the EU institutions. In particular, this option could serve to:

- ensure that the ECD applies to OPs offering their services for free or under the 'freemium/premium model', as well as cases where users' personal data represent a de facto counter-performance;
- ensure that the ECD applies to OPs, such as cloud computing and storage, online advertising platforms, and collaborative platforms, allowing their activity to fall under the notion of 'hosting' as per Article 14 ECD;
- clarify whether activities such as ranking, indexing, provision of review systems etc. are of 'active nature' and thus prevent the OPs from relying on the exemption under Article 14 ECD; alternatively, the distinction could be removed, so as to apply the liability exemptions to all providers of digital intermediation services, both passive and active;
- clarify that the adoption of pro-active measures to fight illegal content online would not make OPs 'active', and deprive them of the liability exemption under Article 14 ECD; alternatively, an express 'Good Samaritan' rule could be adopted;
- clarify what constitutes 'actual knowledge' or 'awareness' of 'illegal content or activity', as well as what reaction to an infringement is deemed 'expeditious';
- clarify the distinction between 'specific content monitoring obligations' and 'general duty of care', to ensure that OPs do not over-remove, fearing liability.

This solution would improve legal certainty, clarifying many critical issues in the application of the ECD and is therefore highly recommended. Ideally, it could be complemented with other initiatives, such as the establishment of sectoral harmonised regimes of liability.

Model B – Establishing a harmonised regime of liability

Under this option, the EU institutions would directly harmonise (at least some of the) conditions under which OPs may be held liable for the illegal content/conduct of their users. In particular:

- OPs could be subject to a specific duty to act whenever they obtain credible evidence of illegal conduct that is to the detriment of other users, as well as take adequate measures to prevent harm. Failure to do so would make them liable for the damages. This option could complement or replace the liability exemption under Article 14 ECD. It could constitute the baseline regime, to be supplemented by sectoral liability rules;
- OPs could be subject to specific sectoral liability regimes. This could occur for damages suffered by users of transaction platforms due to the defective/harmful nature of the product/service offered by other users. It could be possible to envisage a form of strict and objective liability under the RMA. Such a solution could be less adequate in cases of damages caused by a breach of peer-to-peer contracts, unless the platform takes up certain responsibility – e.g. warranties on the quality and security of the transaction – where the reduced capacity to manage risks would create suboptimal incentives in policing users' activities. OPs may be obliged to ascertain the reliability of their users, and cooperate in identifying the infringer.

Clear conditions for liability may provide greater certainty and safety for companies, users and society alike, in a more effective manner than a general duty of care entails, while setting a level playing field for OPs across Europe. Moreover, case-by-case provisions of OPs' duties and corresponding liabilities under an RMA could substantially improve user protection, further clarifying the applicable legal framework, and thereby ensuring maximum legal certainty.

Modification of OPs' secondary liability is therefore highly recommended and, indeed, because of the associated greater legal certainty and uniformity, constitutes the preferred solution. This, however, would in no way prevent policy-makers from adopting it in combination with other solutions, to create positive synergies among the various policy options proposed.

Table of Contents

Executive summary III

List of abbreviations XV

List of tables XVII

1. Introduction 1

2. Methodology and resources used 4

3. EU initiatives and policy background 5

4. Platforms: business models, definitions and classification 7

4.1 Lack of an established definition and need to develop a classification of platforms 7

4.2 A *prima facie* description of platforms and the delimitation of the object of the study 11

4.3 Mapping platforms: a proposed classification 16

5. Liability of online platforms 24

5.1 Types and functions of liability rules 24

6. Applicable framework: identification, analysis and assessment 27

6.1 e-Commerce Directive and the platform's intermediary liability 28

6.2 Media Law 34

6.3 Online piracy, IP and copyright infringements 37

6.4 Child Protection 43

6.5 Hate Speech 47

6.6 Disinformation and voting manipulation 51

6.7 Extremist/terrorist content 55

6.8 Unsafe Products 58

6.9 Other forms of liability: Contractual Liability 63

6.10Other forms of liability: Data protection 68

7. Latest policy initiatives in regulating online platforms' liability 70

8. Policy options 72

8.1 General considerations guiding the identification and assessment of the policy options 73

8.2 Suggested Policy Options 74

9. Conclusions 84

10.References 90

Annex 1 - EU policy initiatives 98

Annex 2 - Legal definitions of online platforms 102

Annex 3 - Regulatory frameworks 130

List of abbreviations

AI	Artificial intelligence
AVMSD	Audiovisual Media Services Directive (EU) 2018/1808
AVMS	Audiovisual Media Services
B2B	Business-to-Business
B2C	Business-to-Consumer
B2G	Business-to-Government
CDSM	Directive on Copyright in the Digital Single Market (EU) 2019/790
Ch.	Chapter
CJEU	Court of Justice of the European Union
C2C	Consumer-to-Consumer
C2G	Consumer-to-Government
EC	European Commission
ECD	e-Commerce Directive 2000/31/EC
EU	European Union/European
ELI MRs	European Law Institute Model Rules on Online Platforms
GDPR	General Data Protection Regulation (EU) 2016/679
GPSD	General Product Safety Directive 2001/95/EC
IAP	Internet access provider
IP	Intellectual property
IPRED	Enforcement Directive 2004/48/EC
ISSP	Information society services provider
ISP	Internet service provider
KPI	Key performance indicator
Member States	Member States
R	Regulation (EU) 2019/1020
NEB	National enforcement bodies
NTD	Notice and take down
OCSSP	Online content-sharing service providers
OCSP	Online content services providers
OTT	Over-the-top

OPs	Online platforms
PLD	Directive 85/374/EEC
PO	Platform operator
P2B	Platform-to-Business
RMA	Risk management approach
SMART	Specific, measurable, attainable and timely
VIC	Vertically integrated companies
VSPS	Video-sharing platform services
UCPD	Directive 2005/29/EC
UK	United Kingdom
US	United States of America

List of tables

Table 1 - From the Digital Market Strategy to the Communication on How to Tackle Illegal Content Online _____5

Table 2 - Commission's Recommendation on Measures to Effectively Tackle Illegal Content Online _7

Table 3 - OPs' Classification _____23

Table 4 - OPs' sources and rules on liability _____86

1. Introduction

Online platforms (OPs), although not an entirely new phenomenon, have gained significant importance in the last decade and the public debate on their responsibilities and liability has reached an unprecedented level.[1] This is the result of the economic power and societal importance they gained, fostered by the new era of digitalisation.

OPs have penetrated all product and service markets and have changed how goods are sold and purchased, and how information is exchanged and obtained, allowing a shift from the offline world to the online environment, where they provide a myriad of digital services.

Hosting platforms have reached a central role in allowing access to and exchange of information, permitting the mass diffusion of any type of content, both legal and illegal. Indeed, their role in the digital realm has morphed, from that of mere hosting providers to that of actors governing how content is displayed and shared online, undertaking certain actions such as moderation, curation and recommendation. This raised pressing questions on their responsibility in preventing the diffusion, detection and subsequent removal of the illegal material shared through their infrastructure.

Moreover, next to plainly illicit material, other harmful content emerged, potentially affecting the social and political discourse, as well as everyday interactions occurring ever more online.

This has led to the need to assess the adequacy and efficiency of the EU extant legal framework, in particular with respect to the e-Commerce Directive (ECD) and the liability exceptions it provides. This, in turn, raised the necessity to understand the correct balancing between the need to ensure active participation of OPs in the fight against illegal/harmful material and behaviour, on the one hand, and the need to ensure users' protection, as well as the protection of their fundamental rights and freedoms, including that of expression, on the other hand.

Finally, the emergence of large OPs or marketplaces, enabling direct interaction between producers and consumers, poses new challenges to product safety, consumer protection, and unfair business practices, raising the issue of the adequacy of the extant legal framework, conceived primarily for traditional businesses and retailers, and overall a less life-pervasive internet.

Against this background, the study, after having linked the key characteristic of platforms with specific policy issues (Chapter 3), undergoes a review of the legal framework, comprised of both hard- and soft-law instruments, as well as voluntary agreements and practices, with respect to different sources of potential liability, assessing its adequacy and effectiveness in light of the policy and academic debate, whenever relevant.

To this end, however, the object of the study – namely the very notion of online platform – is discussed in greater details (see section 4.1). Indeed, this notion is used in a variety of ways to indicate extremely broad and diversified sets of services and tools (see section 4.2).

[1] For the policy debate, see Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy available at https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud; European Commission (2016). Communication from the Commission. Online Platforms and the Digital Single Market Opportunities and Challenges for Europe. COM(2016) 288 final Brussels, European Commission. , European Commission (2017). Communication from the Commission. Tackling Illegal Content Online. Towards an enchanced responsibility of online platforms. COM(2017) 555 final Brussels, European Commission, European Commission (2018). Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online. C(2018) 1177 final Brussels, European Commission.

Against this background, the study attempts to give a first delimitation of the object of inquiry, and then to categorise OPs pursuant to multiple criteria, namely: (i) the activities and functions they serve; (ii) the actors they involve and the ways in which they interact with them in their operation; (iii) their different sources of revenue and associated business models; (iv) the way in which they use and exploit data; (v) the level of control they exercise on users' activities; and (vi) possible types of infringements carried out through their infrastructures and associated harms. Absent a unique and definitive definition of OPs – which would be conceptually impossible and practically useless – [2] the classification proposed is indeed intended to offer the basis for a flexible taxonomy of OPs, to be carried on a case-by-case-basis, in light of the specific social and regulatory issues to be addressed, under a bottom-up, technology-specific and functional approach (see section 4.3.1).

The study then moves on to analyse the responsibility and liability of OPs starting with that related to illegal and/or harmful material, made available on, uploaded or shared on the platform, as well as for transactions occurring on it. In doing so, the study sets forth a clear conceptual framework by analysing the difference between responsibility and liability, and the different types of liability, distinguishing, on the one hand, between civil, criminal and administrative liability and, on the other hand, between strict, semi-strict or fault-based liability (see section 5.1).

In particular, in section 6.1, the e-Commerce Directive's relevant provisions are analysed and possible shortcomings resulting from its sometimes divergent application in Member States are highlighted, together with those arising from the uncertain application of the notion 'information society services' to new types of OPs, the unclear boundaries between 'active' and 'passive' providers, the lack of a 'Good Samaritan' clause, as well as the ban on a general duty to monitor and its compatibility with Member States' legislation or case-law ordering OPs to take certain proactive monitoring measures.

Then, in section 6.2 the media law regulatory framework is addressed, with particular reference to the Audiovisual Media Services Directive,[3] with an emphasis on the benefits it provides, as well as on its lacunae, such as the lack of clarity around the regulated actors ('video-sharing platform services providers'), and the limited scope of application with respect to only certain types of online harmful content, namely, those related to children protection, hate speech and extremist content.

In section 6.3 the study maps the applicable framework for IP rights infringements carried out on or through the OPs' infrastructures, both of a mandatory and voluntary nature, assesses the innovations made by the new Copyright in the Digital Single Market Directive, especially the liability provisions under Article 17, and provides an account of the possible tensions arising between such rules imposing a more extensive monitoring obligation on OPs and the ban on general monitoring provided under Article 15 of the ECD (see section 6.3).

In section 6.4 the framework applicable to the protection of children against both thematic and associated online harms is analysed, and the main tendencies and problematic issues associated thereof are presented such as a preference over self-regulatory and user-empowerment solutions, legal fragmentation and lack of clear obligations for OPs.

[2] Similarly see Lambrecht, Verdoodt and Bellon (2018). 'Platforms and commercial communications aimed at children: a playground under legislative reform?' International Review of Law, Computers & Technology **32**(1): 58-79 and Gawer (2016). Online Platforms: Contrasting perceptions of European stakeholders A qualitative analysis of the European Commission's Public Consultation on the Regulatory Environment for Platforms.

[3] See Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), *OJ L 95, 15.4.2010, p. 1–24.*

In section 6.5, OPs' responsibilities are mapped and analysed with respect to hate speech proliferated or undertaken on their infrastructure, based on EU's and Germany's legislation and on the extant voluntary instruments such as the Code of Conduct on Countering Illegal Hate Speech Online.[4] The efficiency and limitations of these instruments are analysed based on existing evidence, which shows, among others, that the issues of lack of transparency around OPs' removal procedures and of OPs' possible content over-removal are still to be considered.

The study analyses in section 6.6 the voluntary initiatives adopted at EU level to tackle disinformation and voting manipulation and provides an overview of two cases where Member States have adopted legislation in this respect. The effectiveness of these instruments is discussed, as both approaches suffer from different limitations, by being either too soft or too stringent.

In section 6.7, OPs' duties to reduce extremist/terrorist content on the infrastructure are indicated and the way they function in practice, together with the current proposal for a regulation on preventing the dissemination of terrorist content online. Extant EU initiatives and reports show that tackling terrorist content is a problem of many hands, which requires a holistic approach and strong cooperation between OPs, national and international organisations, stakeholders and members of the society. Yet, again, setting stringent blocking and removal obligations on OPs, especially if not associated with adequate safeguard mechanisms, may result in an undue limitation on users' fundamental rights and freedoms, and needs to be carefully assessed.

The proliferation of online marketplaces related to digital services raises concerns with respect to the circulation of unsafe products and creates new challenges for market surveillance authorities in a digital environment. These challenges and the need therefrom for OPs to boost their efforts and improve their uptake of risk-reducing measures, together with product safety, liability and surveillance legislation and international case-law are being analysed in section 6.8.

Then, section 6.9 provides an analysis from a contractual and consumer protection point of view of the regulatory framework applicable to P2C, P2B and C2C relations and the emerging challenges associated with, among others, the unclear qualification of the parties (such as in the case of prosumers) and the OPs' superior bargaining power and the possibility to impose unfair terms on their users. After having highlighted possible regulatory gaps, current initiatives on the regulation of the OPs' relationships with their users are discussed.

As OPs' business models and users' activities pose not only personal data protection risks, but also associated risks such as the creation of filter-bubbles, micro-targeting and sometimes harmful manipulation, the users' safeguards and OPs' obligations under the General Data Protection Framework are analysed in section 6.10. Then, a brief overview of the latest policy initiatives in regulating OPs is provided under Chapter 7.

Finally, taking into account the aforementioned overall granular analysis, the study presents in Chapter 8 feasible and realistic policy options, – assessed against suitable performance criteria i.e. their costs and benefits, feasibility and effectiveness, sustainability, risks and uncertainties, cohesion with EU objectives and ethical, social and regulatory impact (section 8.1- 8.2)– namely: (i) maintaining the status quo (see section 8.2.1); (ii) promotion of awareness-raising and media literacy campaigns (section 8.2.2); (iii) promoting self-regulation (section 8.2.3); (iv) establishing co-regulation mechanism and tools (section 8.2.4); (v) adopting statutory legislation (section 8.2.5) either by (vi) establishing clear and narrow tailored primary duties for OPs (see §1)a)i)8.2.5.1); or by (vii) modifying OPs' secondary

[4] See *The EU Code of conduct on countering illegal hate speech online*, 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.

liability by employing two different models (see §1)a)i)8.2.5.2), that is (a) by clarifying the conditions for liability exemptions under the ECD 'Safe Harbour' or (b) by establishing a harmonised regime of liability.

2. Methodology and resources used

Since the purpose of this study is to analyse the rights, roles and responsibilities of OPs and the main legal/regulatory challenges associated with their operation, after providing a conceptual framework by distinguishing between responsibility and liability of OPs, the differences thereof and the different types of liability (see section 5.1), a desk research was conducted to identify and assess all the relevant applicable regulation, as well as soft law and self-regulatory instruments.

For each of the relevant issues identified, namely:

- the e-Commerce Directive and the Platform's Intermediary liability (see section 6.1);
- harmful and illegal content on social media and video streaming platforms (see section 6.2);
- online piracy, IP and copyrights infringements (see section 6.3);
- the protection of minors in the OPs ecosystem (see section 6.4);
- online hate speech (see section 6.5);
- disinformation and voting manipulation (see section 6.6);
- extremist and terrorist content online (see section 6.7);
- the sale and circulation of unsafe products on the internet (see section 6.8);
- contractual liability in P2C, P2B and C2C relations (see section 6.9);
- user safeguards and OPs' obligations with respect to the protection of personal data under the GDPR (see section 6.10);

The relevant EU applicable legislation and case-law were considered, together with voluntary initiatives (such as Codes of Conducts and Memoranda of Understanding), where appropriate. At times, reference was made also to pertinent Member States' legislation, without, however, undergoing a systematic comparative analysis that fell beyond the purpose of the study.

For each issue, after providing a synthetic overview of the applicable regulatory background (comprised of both hard and soft law tools), a discussion is conducted isolating the most relevant regulatory and policy issues emerging from the application of said norms to the relevant kind of OPs. Such discussion takes into account relevant policy documents issued by EU and other prominent institutions (e.g. OECD), as well as reports and scholarly work.

Literature was first identified through targeted searches of relevant academic journals, and online databases.

Subsequently, additional literature in the form of reports and studies carried out at EU and international level was identified and analysed. Said materials differ in nature and approach, but may be categorised as follows: (i) reports from the EU Institutions including in-depth analysis of consultation procedures, stakeholders views, synopsis of the application of the extant regulatory framework at EU and Member State level, statistical and factual assessments of the practical implementation of voluntary initiatives, etc.; (ii) legal and economic reports and studies carried out by experts and academic stakeholders for the EU Institutions; and (iii) international reports having a similar methodological approach as the reports under (i) and (iii).

On the basis of the above referred analysis, policy options were formulated that are relevant for the issue of OPs' liability taking into account their expected impact, functionality and time scale.

3. EU initiatives and policy background

The European approach. Concerns on the spread of illegal/harmful material online – ranging from incitement to terrorism, hate speech and child sexual abuse, to infringement of intellectual property (IP), privacy and consumer protection – are shared at the EU, national and international level, with legal scholarship and policy makers advocating for OPs to play a more active role in fighting illegal and harmful content, owing to the economic and regulatory powers gained by them in the last years.[5]

In the EU, several steps have been taken on the regulation of OPs and their liability for the diffusion of illegal/harmful content online, with a series of non-binding policy documents shaping what might be defined as the 'European approach', to be briefly summarised below.

Indeed, since they constitute the conceptual framework necessary to understand the rationales and aims of subsequent policy intervention, said documents shape the regulatory framework, both as sources of soft-law and as tools to interpret the legislative and non-legislative instruments adopted in their aftermath. In this sense, they (i) allow the identification of the applicable rules shaping OPs' rights, duties and liabilities, also taking into account how and why the current *status quo* was reached –, and (ii) constitute a benchmark against which the adequacy and effectiveness of said legal rules in tackling illegal/harmful content online may be assessed.

Table 1 - From the Digital Market Strategy to the Communication on How to tackle illegal content online

From the Digital Market Strategy to the Communication on How to Tackle Illegal Content Online	
Sector-specific and problem-based regulatory approach	Given the difficulty and limited purposefulness of a one-size-fits-all understanding, EU Institutions agreed that OP should be distinguished and defined in their relevant sector-specific legislation at EU level according to their characteristics, classification and principles and following a problem-driven approach, committing to a sector-specific and problem-based approach to their regulation.[6]
Removal of barriers and level playing field	EU Institutions aim to address the barriers hindering the growth of the online economy, creating a level playing field, both between online and offline services, and among different services offered by different platforms. They advocate for tailor-made solutions, to ensure fair competition and equal footings (e.g. size), avoid monopolies or abuse of dominant position.[7]
High level of users' protection and empowerment	High protection of OPs' users is fundamental, as well as extensive information to and empowerment of members of the civil society. Technical solutions shall ensure compliance with the relevant legislation, and cooperation among authorities. Particular attention is granted to ensuring correct review systems, and platforms are urged to adopt clear comprehensive and fair terms and conditions, high standards of consumer protection also in consumer-to-consumer (C2C) relations, and transparency measures on the criteria used to filter, rank, sponsor, personalise and or review information presented to users.[8] Lack of transparency and fairness in business-to-business (B2B) relations is highly problematic, and targeted legislative intervention on the matter was called for.[9] Clear thresholds for assessing whether collaborative economy OPs' users qualify as professionals or consumers are necessary, to clarify the scope of application of consumer protection law both in the users' transaction and in their relationship with the platforms, as well as the platforms' liability when problems in the peers' transaction arise.[10]

[5] See European Commission (2020). Communication from the Commission. Shaping Europe's digital future. COM(2020) 67 final Brussels, European Commission, p. 11, COM(2017) 555 final. European Commission (2016). Communication from the Commission. A European agenda for the collaborative economy. COM(2016) 356 final Brussels, European Commission, p. 9.

[6] See Wiewiórowska-Domagalska (2017). Online Platforms: How to Adapt Regulatory Framework to the Digital Age? Briefing PE 607.323., p. 5.

[7] See COM(2016) 288 final., p. 5, COM (2020) 67 final, pp. 2 and 8.

[8] See European Parliament (2017). European Parliament resolution of 15 June 2017 on online platforms and the digital single market (2016/2276(INI))., para. 48-62.

[9] Against this background, the European Parliament and the Council adopted the Regulation (EU) 2019/1150 of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, PE/56/2019/REV/1, OJ L 186, 11.7.2019, p. 57–79.

[10] See COM(2016) 356 final. pp. 2 and 9-10.

	Effective and transparent trust-building mechanisms (e.g. review systems) are seen as a possible alternative to legislation, especially in the case of peer-to-peer transactions.
Re-distribution of wealth for IP and copyright owners	EU Institutions stressed the need for measures that could re-balance the unfair allocation of value deriving from the distribution of creative content due to the uncertain status of online services under copyright and e-commerce law. On this matter, it was suggested that OPs on which a significant volume of protected work are stored and made available to the public – unless 'passive', and thus covered by the exemption in Article 14 of the so-called e-Commerce Directive[11] (ECD) – should conclude license agreements with relevant right holders, to ensure fair profit-sharing with authors, creators and relevant right holders.[12]
Tackling illegal content online – shared responsibility and direct platform's involvement	Since 'what is illegal offline is illegal online', EU Institutions recognised that OP 'which mediate access to content for most internet users carry a significant social responsibility in terms of protecting users and society at large and preventing criminals and other persons involved in infringing activities online from exploiting their services', and thus 'should decisively step up to address this problem, as part of the responsibility which flows from their central role in society',[13] which also covers the need to balance the fight against illegal content and protection of the different fundamental rights at stake.[14] Indeed, a balanced approach is advocated: legal certainty and shared allocation of responsibility could strengthen the platform economy, while providing adequate incentives for all the actors involved (OPs, users' and consumers' associations, individual users, national and EU law-enforcement and supervision authorities, and society at large) to fight illegal content online.
Maintain intermediaries' exemption of liability, while promoting OPs' proactive involvement in tackling online illegal/harmful content	Taking account of the results of the consultations on the regulatory environment for platforms, both the Commission and the Parliament have so far showed support for the current framework contained in the ECD (see section 6.1), but also highlighted the need to clarify the liability regime as to allow platforms to comply with the current framework, eliminate certain flaws in its enforcement, and complement it with further measures to ensure an effective detection, removal and prevention of online illegal/harmful content.[15] Particular rules and procedures are envisaged for serious crimes or offences.

Commission's recommendation on measures to effectively tackle illegal content online. As for the latest sets of goals, the Commission prompted Member States and OPs to adopt suitable measures to ensure quick and proactive detection, removal and prevention of reappearance of illegal content, thus increasing the platforms' responsibility in the governance of online material, without affecting the liability regime set out in the ECD.[16]

[11] See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1-16.

[12] Against this background, the European Parliament and the Council adopted the Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, pp. 92-125).

[13] See COM(2017) 555 final., p. 2.; COM(2016) 288 final.

[14] See COM(2017) 555 final., p. 3.

[15] See European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI)), para. 29-41.

[16] See C(2018) 1177 final.

Table 2 - Commission's Recommendation on Measures to Effectively Tackle Illegal Content Online

Commission's Recommendation on Measures to Effectively Tackle Illegal Content Online.	
Detecting and notifying illegal content, in cooperation with competent authorities	OPs should systematically enhance their cooperation with competent authorities in Member States: evidence of criminal offences obtained in the context of removal should be transmitted to law enforcement authorities, in compliance with the law; competent authorities should ensure that courts can effectively react to illegal content online, and enable stronger cross-border cooperation. Effective points of contact should be established, and digital interfaces set up for cooperation. OPs shall grant cooperation tools and information exchange to trusted flagger, possibly agreeing on EU-wide criteria for their identification. They should establish easy, accessible, user-friendly and high-quality notification mechanism, allowing swift and informed follow-ups. Use of proactive measures for detection – including automatic tools and anti-re-upload-systems – shall be incentivised. Their use shall not *per se* make the platform 'active', leading it to lose the liability exemption under the ECD.
Removing illegal content	OPs must take down illegal content expeditiously once they become aware of its existence to avail of that exemption set out in Article 14 ECD. Promptness is paramount where serious harm is at stake (e.g. incitement to terrorism) and may require fixed timeframes. OPs should explain in a clear, easy, sufficiently detailed and understandable manner in their terms of service the type of content permitted/non permitted, and what are the procedures for contesting removal decisions. OPs should publish detailed transparency reports, at least once per year. Finally, OPs should offer safeguards against over-removal and abuse of the system, with simple online counter-notice procedures and reasoned follow up, using, when possible, out-of-court dispute settlement.
Preventing the re-appearance of illegal content	OPs shall take measures to refrain users from repeatedly uploading illegal content of the same nature; thus, use and development of automatic tools are encouraged, provided that they are transparently described in the OPs' terms of services and accompanied by a reversibility safeguard. Access to relevant databases (e.g. Database of Hashes) should be available to all OPs.
Clearer 'notice and take down action' procedures.	OPs shall provide easy and transparent rules for notifying illegal content and fast-track procedures for 'trusted flaggers'. At the same time, they shall inform content providers and allow them to contest the action, eventually avoiding the (over)removal of licit content.
More efficient tools and proactive technologies	OPs shall provide clear notification systems and proactive tools for detection and removal, in particular where content is potentially highly harmful and does not require contextualisation (e.g. terrorism and child sexual abuse, counterfeited goods). They shall implement measures to effectively reduce the uploading and sharing of terrorist propaganda (prohibition to host terrorist content; 1-hour removal).
Stronger safeguards to ensure fundamental rights	OPs shall put in place effective and appropriate safeguards, including human oversight and verification where automated tools and filters are used, to ensure that removal decisions are accurate, well-founded and fully respectful of fundamental rights.
Special attention to small companies	OPs shall adopt voluntary arrangements, tools for sharing experiences and best practices, as well as technological solutions, enabling automatic detection, to benefit smaller platforms, which may lack the necessary resources and experience to adopt a higher degree of governance in the field.

4. Platforms: business models, definitions and classification

4.1 Lack of an established definition and need to develop a classification of platforms

Need to define the object of the study and lack of established definitions. A study on OPs' liability cannot be undertaken, without a prior definition of the object of the inquiry. Said otherwise, to describe and assess OPs' liability we first need to understand exactly what the latter are. However, there is no

consensus on a single definition of OPs, neither in computer science nor in the economic and legal domain.[17]

The EU choice not to have a definition of 'OPs' and the adoption of a 'sector-specific approach'. Indeed, the EU expressly chose not to adopt one clear-cut definition of OPs, and rather to rely on the sector-specific notions set out in the existing legislation (see Chapter 6). In its 2017 Resolution, the European Parliament claimed that 'it would be very difficult to arrive at a single, legally relevant and future-proof definition of online platforms at EU level, owing to factors such as the great variety of types of existing online platforms and their areas of activity, as well as the fast-changing environment of the digital world', stating that 'in any case one single EU definition or "one size fits all" approach would not help the EU succeed in the platform economy'.[18] It ultimately argued that 'online platforms should be distinguished and defended in a relevant sector-specific legislation at EU level according to their characteristics, classifications and principles and following a problem-driven approach'.[19]

Support for the EU approach. Need for a tentative definition and a modular classification of OPs as a conceptual tool. The position is to be welcomed. One, all-encompassing legally binding definition is impossible to conceive and would either 'miss certain online platforms, or conversely apply to a very wide range of Internet services',[20] and thus be detrimental from a legal and policy-making point of view.

However, the discussion on how OPs are structured and how they may be classified shall not be dismissed, provided that few methodological and theoretical *caveats* are set.

On the functional approach on legal concepts in Law and Technology. There is a bi-directional relationship between policy interests and the definitions of the entities to be regulated, on the one hand, and between said definitions and the characteristic displayed by such entities, on the other hand.

In the field of Law and Technology, many notions are elusive and indeterminate, being used with different meanings in a variety of contexts. Notions such as 'robotics' and 'AI' have a common understanding which has limited descriptive capacity, and might even be misleading if used for normative purposes. At the same time, more precise definitions offered by researchers display a greater precision, but offer a fragmented and contradictory picture, because they respond to the specific perspective and background of the individual speaker, and thus prove unworkable for broader policy purposes.[21] Furthermore, the diversity of the technical features displayed by the various robotics

[17] See European Commission (2016). Commission Staff Working Document. Online Platforms Accompanying the document Communication on Online Platforms and the Digital Single Market. SWD(2016) 172 final Brussels, European Commission. , p. 2. OECD (2019). 'An Introduction to Online Platforms and Their Role in the Digital Transformation of Entry.' An Introduction to Online Platforms and Their Role in the Digital Transformation of WebLog https://www.oecd-ilibrary.org/content/publication/53e5f593-en 2019., p. 20. Martens (2016). An Economic Policy Perspective on Online Platforms. Institute for Prospective Technological Studies Digital Economy Working Paper 2016/05, Studies. , p. 3.

[18] See European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI))., para. 6-7.

[19] See ibid., para. 8. The same was stated in SWD(2016) 172 final., p. 2., where it is stated that 'online platform is a broad label for numerous types of multi-sided business models', and 'even at a theoretical level, depending on the definition, online platforms are a flexible concept. Furthermore, they are continuously changing and developing in new directions'. The European Commission then acknowledged the policy-implications: 'it is challenging to set out a clear-cut definition of online platforms, especially from a legal perspective. Doubts have been raised during the stakeholder engagement process over whether any 'one size fits all' definition would be feasible. Such a definition is unlikely to be future-proof and it might overlap with other definitions, for example that of an online intermediary and information society service providers'.

[20] See SWD(2016) 172 final., p. 1.

[21] See Bertolini (2013). 'Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules.' Law Innovation and Technology **5**(2): 214–247. Palmerini, Azzarri, Battaglia, Bertolini, Carnevale, Carpaneto, Cavallo, Di Carlo, Cempini, Controzzi, Koops, Lucivero, Mukerji, Nocco, Pirni, Shah, Salvini, Schellekens and Warwick (2014). Guidelines on Regulating Robotics. Erica Palmerini et al., 'Robolaw: Towards a European Framework for Robotics Regulation,' Robotics and

applications, as well as of the use for which they are developed and deployed, is such that notions like 'robot' can only work as a broad label, synthetically indicating an extensive set of objects.[22] Having a non-technical nature, these notions can be defined to include all the possible devices that are still considered to belong to them,[23] thus displaying no normative value from a conceptual, and, eventually, from a legal perspective.

Mutatis mutandis, the same can be said about OPs. Science-engineers commonly use this term to denote a set of technologies or interfaces available to a broad base of users who build processes, applications, technologies and business models with it and on it.[24] On the contrary, social scientists, policymakers, as well as the general public, normally employ it to indicate triangular digital infrastructures allowing interactions between different subjects and actors, covering – by extension – (i) the infrastructure itself (ii) the entity (legal subject) who runs it, and (iii) the economic model adopted by the latter. Under this approach – which primarily focuses on the economic structure realised OPs are described as 'software-based facility[ies] providing two – or multi-sided markets where providers and users of content, goods and services can meet',[25] and understood as 'a broad label for numerous types of [digital] multi-sided business models'.[26]

However, just as in the case of 'robotics' and 'AI', it is not the fact that OPs represent a *genus* that makes the term normatively void. Rather, this indeterminacy is due to the inherent difficulty in identifying the *trait d'union* among the different entities that are normally associated with the term. As the EU Parliament acknowledged, OPs vary in the number and types of subjects involved, the activities performed on the platforms by said actors, the activities performed by the platform itself to allow or facilitate the interaction, their sizes, their position on the market, their sources of revenue, and so on.[27] Moreover, their variables are always evolving, together with the development of new business models and technical solutions, so that the characteristics of OPs are constantly changing. Thus, OPs constitute a heterogeneous phenomenon, whose qualifying features are everything but obvious.

For these reasons, rather than one, universally valid definition, we can only develop and work on a classification based on a variety of criteria, while a stipulative notion could only be elaborated to represent the different combination of said variables.[28]

Autonomous Systems 86 (2016). Bertolini (2020). Artificial Intelligence and Civil Liability Bruxelles, Policy Department for Citizens' Rights and Constitutional Affairs.

[22] See Palmerini, Azzarri, Battaglia, Bertolini, Carnevale, Carpaneto, Cavallo, Di Carlo, Cempini, Controzzi, Koops, Lucivero, Mukerji, Nocco, Pirni, Shah, Salvini, Schellekens and Warwick (2014). Guidelines on Regulating Robotics, Palmerini, Bertolini, Battaglia, Koops, Carnevale and Salvini (2016). 'RoboLaw: Towards a European framework for robotics regulation.' Robotics and Autonomous Systems **86**: 78-85.

[23] See Palmerini, Azzarri, Battaglia, Bertolini, Carnevale, Carpaneto, Cavallo, Di Carlo, Cempini, Controzzi, Koops, Lucivero, Mukerji, Nocco, Pirni, Shah, Salvini, Schellekens and Warwick (2014). Guidelines on Regulating Robotics, Palmerini, Bertolini, Battaglia, Koops, Carnevale and Salvini (2016). RoboLaw. Bertolini (2013). Robots as Products.

[24] See SWD(2016) 172 final., p. 32. OECD (2019). An Introduction to Online Platforms., p. 20.

[25] See Obergfell and Thamer (2017). '(Non-)regulation of online platforms and internet intermediaries – the facts: Context and overview of the state of play.' Journal of Intellectual Property Law & Practice **12**(5): 435–441., p. 436.

[26] See SWD(2016) 172 final., p. 45. Here – as it will be clarified in § 4.2 – the technical features (the presence of a digital structure or architecture which could be accessed by different sets of users) are essential but not sufficient for the existence of online platforms. Despite the lack of a set-in-stone business models, platforms stand out for the activities they carry out and enable, and their operation in the digital environment is an additional element to be taken into consideration, because of the way it shapes said activities and the broader effects that platforms have on society.

[27] See COM(2016) 288 final.; European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI)). Also see (§ 4.3).

[28] See Palmerini, Azzarri, Battaglia, Bertolini, Carnevale, Carpaneto, Cavallo, Di Carlo, Cempini, Controzzi, Koops, Lucivero, Mukerji, Nocco, Pirni, Shah, Salvini, Schellekens and Warwick (2014). Guidelines on Regulating Robotics, Palmerini, Bertolini, Battaglia, Koops, Carnevale and Salvini (2016). RoboLaw.

In this sense, the constructions of the classification and the elaboration of the respective general definition are only theoretically distinguishable, whereas, in practice, they feed onto one another, and shall thus be carried out in parallel. A first tentative definition is needed as a practical baseline for identifying and limiting the object of the study. This will then allow to develop a conventional classification of their most important features and characteristics, which could work as a conceptual framework for policymakers, allowing a modular and functionally based categorisation and definition of specific types of online platforms, for different policy interventions. The classification works as a tool to spot – at a given time – the recurring characteristics of OPs, thus helping identify and update the definition elaborated as a starting point, to represent the different combination of said variables and add conceptual clarity to the debate on OPs. Finally, this second definition – which has a merely descriptive nature and should not be directly translated into a legally relevant definition – represents a conceptual tool in itself, as it offers an external critical tool for analysing and rationalising the current legal framework and allows a common understanding of the phenomenon, avoiding the confusion caused by concurrent and non-coordinated notions of platforms.

Indeed, the heterogeneous nature of OPs is mirrored by the variety of notions used in the economic, legal and policy-making discourse (information platforms, service providers, hosting platforms, transaction platforms, e-commerce intermediaries, participative networking platforms, communication platforms, collaborative platforms, information society service providers, etc.). This may prove problematic: in particular, it makes difficult to ascertain whether said notions are intended as (i) mere synonymous of 'online platforms' as a *genus*; (ii) specific subcategories of the latter – and, if so, upon which basis their classification is justified –, or (ii) a broader category, including entities not commonly referred to as platforms (e.g. internet access providers, IAP).[29]

Instead of having a workable set of definitions within 'sector-specific legislation at EU level according to their characteristics, classifications and principles and following a problem-driven approach'[30] – as suggested by the EU Parliament – we have a myriad of uncoordinated definitions, a series of complex cross-reference, and even not-defined notions that necessarily call for an interpretation based on common understanding.[31] As a result, 'when different people are talking about platforms, they have a totally different understanding'.[32] This, in turn, makes it hard for the stakeholders directly involved to correctly identify the applicable legal frameworks, as well as for regulators to assess its effectiveness and eventually formulate adequate policy proposals.

Thus, the conceptual tools that this study aims to elaborate could help legal scholars and policy makers alike to cluster and compartmentalise platforms giving rise to similar social issues, to assess the current legal framework and possibly guide future policy interventions.

As section 4.3 will demonstrate, the heterogeneous nature of OPs makes it impossible to unitarily address the matters they give rise to, since diverse features lead to possibly different social, economic and legal issues, while no technical aspect alone justifies the adoption of ad-hoc regulation. Their inherent differences cannot be overlooked when addressing their regulation, especially when discussing their liability regime. Said otherwise, rather than a 'law of platforms', trying to address the

[29] Perset (2010). The Economic and Social Role of Internet Intermediaries, OECD., p. 9-14.

[30] See European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI))., para. 8.

[31] See for example Directive (EU) 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 L 136, 22.5.2019, p. 1–27. Recital 18 refers to 'platform providers' which may or may not be considered as traders for the supply of digital content or digital services to the consumer but fails to explain what it means by that.

[32] OECD (2019). An Introduction to Online Platforms, p. 20.

phenomenon unitarily,[33] the EU shall aim at adopting a case-by-case analysis of different digital structures according to a functional perspective, i.e. being guided by policy and public interest arguments raised by their functionalities rather than technological considerations (see Chapter 8).

Against this background, in the second part of the study, after having linked the key characteristic of platforms with specific policy issues, a review of the legal framework applicable to each matter shall be undertaken, assessing its adequacy and effectiveness, as the basis for finally elaborating policy recommendations to address existing problems (Chapter 6).

4.2 A *prima facie* description of platforms and the delimitation of the object of the study

The economic perspective as the mainstream approach in the study of online platforms. OPs stand out for the activities they carry out and enable, and by the fact that they operate digitally. Thus, they are mainly qualified according to the specificity of the business model adopted, and the most common approach in their analysis is indeed economic.[34]

According to the economic perspective, OPs are 'matchmakers' that attract two or more types of customers or groups – the sides of the platforms – by enabling them to interact with each other on attractive terms. Depending on the platform in question, said 'users' might be represented by buyers, sellers, renters, workers, app-developer, advertising companies, etc.[35]

This approach is broadly adopted in both the scholarly literature and the policy-making domain. Indeed, the Commission used it, stating that one of the OPs' shared features is that 'they operate in *multisided markets* but with varying degrees of control over direct interactions between groups of users'.[36] Many other policy documents, both at the national, international and European level, despite either not engaging into an express description of the phenomenon considered,[37] or adopting definitions that do not overlap with one another,[38] seem nevertheless to start from a business-based understanding of what makes something an OP.

[33] In her political guidelines, the President of the European Commission, Ursula von der Leyen, has committed to upgrade the Union's liability and safety rules for digital platforms, services and products, with a new Digital Services Act. See von der Leyen (2019). A Union that strives for more. My agenda for Europe by candidate for President of the European Commission. Political Guidelines for the Next European Commission 2019-2024. , available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[34] See, e.g.: OECD (2019). An Introduction to Online Platforms.; Perset (2010). The Economic and Social Role of Internet Intermediaries.

[35] See Evans and Schmalensee (2016). 'Matchmakers: The New Economics of Multisided Platforms of Entry.' Matchmakers: The New Economics of Multisided Platforms of WebLog https://books.google.it/books?id=plhZCwAAQBAJ 2016., Kindle file. 'Matchmakers are called multisided platforms because they usually operate a physical or virtual place that helps the different types of customers get together'. Also see OECD (2019). An Introduction to Online Platforms., p. 21; SWD(2016) 172 final., p. 1.

[36] See COM(2016) 288 final. p. 2 (emphasis added). The aforementioned Commission's definition of platforms is similar to the one used by Ecorys in a study for the EU Parliament. In this sense, see Van Gorp and Batura (2015). Challenges for Competition Policy in a Digitalised Economy. Study for the ECON Committee Brussels, Policy. , p. 7-8: 'A platform provides a (technological) basis for delivering or aggregating services/content and mediates between service/content providers and end-user'.

[37] Often online platforms are described merely by means of exemplification. See for example: 'online platforms (e.g. search engines, social media, e-commerce platforms, app stores, price comparison websites, ad networks) play an ever more central role in the online world and hence in social and economic life' in SWD(2016) 172 final. p. 1.

[38] See Annex I.

Typical features of platforms according to the economic perspective. Indeed, OPs are often described through a series of relevant characteristics:[39]

- Their capacity to facilitate and create added value from interactions and transaction between users, according to a non-linear business model;
- Their capacity to collect and process large volume and variety of data to improve their business (so-called 'economy of scope');
- The positive correlation between the increase of users or the users' activities on the platforms and the optimisation of their services and utility for the users' themselves (so-called 'network effect', which can be either direct – when the utility the users on one side derive depends on the number of users on that same side, as in the case of social media – or indirect – when a group of users benefits more as the users in the other group increase, such as in online marketplaces);[40]
- Their tendency to drastically alter markets or create new ones (disruptive nature).

These features are often identified in the majority of platforms, but not in all of them. Thus, 'certain characteristics (such as network effects and use of data) are more pronounced and relevant in many platform cases, but this does not warrant a delineation of digital platforms through a specific definition',[41] so that these features are reflecting the different economical and revenue/pricing strategies adopted, rather than constitutive elements necessary for determining whether something qualifies as an online platform.[42]

The mainstream definition: OPs as digital infrastructures allowing multisided interaction. In the economic literature, there seems to be a consensus on the fact that OPs are a peculiar digital version of traditional off-line platforms – i.e., physical marketplaces –, which are characterised by two key elements: they are *multisided*, and they *facilitate interactions*.

Building on a report on Online Platforms and Their Role in the Digital Transformation issued by the OECD in 2019 – which mirrors many other policy documents and studies produced so far –, the economic-based definition of OPs may be summarised as follows: OPs constitute 'digital service[s] that

[39] See for example SWD(2016) 172 final., p. 2, where the European Commission refers to the following important characteristics: 'capacity to facilitate, and extract value, from direct interactions or transactions between users; ability to collect, use and process a large amount of personal and non-personal data in order to optimise, *inter alia*, the service and experience of each user […]; capacity to build networks where any additional user will enhance the experience of all existing users […]; ability to create and shape new markets into more efficient arrangements that bring benefits to users but may also disrupt traditional ones: reliance on information technology as the means to achieve all of the above.

[40] To these essential features, others are sometimes added, namely: OPs' capacity to grow without increasing the investments in tangible assets or workforce (so call ability to scale without mass); their potentially global reach; their ability to benefit from the complementarities that may exist between the services they provide, (so called panoramic scope, which is particularly relevant for super-platforms); their capacity to benefit from – and possibly purposefully increase – the costs the users shall sustain in order to switch to competitors, as to ensure fidelity od their customers (e.g. increasing switching costs for the purpose of ensuring that customers are 'single-homing'); their capacity to impose themselves as monopolist forces on the marker, due to the joined operation of all the features discussed above (so called winner-takes-all or winner-takes-most effect). See in this respect OECD (2019). An Introduction to Online Platforms., pp. 22-25; Evans and Schmalensee (2010). 'Failure to Launch: Critical Mass in Platform Businesses.' Review of Network Economics **9**(4)., pp. 21-23.

[41] See van Eijk, Fahy, van Til, Nooren, Stokking and Gelevert (2015). Digital platforms: an analytical framework for identifying and evaluating policy options The Hague. p. 46.

[42] E.g. online platforms may choose to exploit the direct and indirect network effects and economies of scale, or even operate without any of the latter or merely one of them. Ibid., Nooren, van Gorp, van Eijk and Fathaigh (2018). 'Should We Regulate Digital Platforms? A New Framework for Evaluating Policy Options.' Policy and Internet **10**(3): 264-301., p. 271.

facilitate interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet' at least in one direction.[43]

From this account, three elements rise as both sufficient and necessary for an entity to qualify as an online platform:

- the entity in question offers a service or a structure that other subjects may use;
- said service or structure operates digitally;
- said service or structure is meant to allow or facilitate interaction among two or more (sets of) users.[44]

In this sense, the third point merges the two key elements mentioned above: the multisided nature of platforms, and their role as facilitators of interactions among their users.

Despite commonly used, this definition may be criticised, and, for defining the object of this study, it shall be reconsidered, as it covers too much and too little at the same time.

The need to overcome a strict interpretation of the concepts of 'multisided nature of platforms' and 'intermediation'. In economic studies, OPs are known as two-sided or multisided markets facilitating the exchange of information or transaction among users, and they are differentiated from traditional pipeline business models precisely because: (i) the value generated by the platform is for the major part generated online by its users, rather than by the supply of a product or service; (ii) they rely on positive network effects. Indeed, many studies emphasise that the presence of strong indirect effect is a fundamental feature distinguishing platform from one-sided markets, with some authors claiming that it is sufficient for one-way indirect network effect to be present to determine the existence of a platform,[45] whereas other go as far as to require both sides to be affected as a necessary condition thereof.[46]

As highlighted by the European Commission[47] and economic studies,[48] this reading might prove problematic because it leads to cut off important online service providers, sharing similar characteristics and/or raising consumer and public interest concerns that cannot be overlooked.

For example, media-services providers and production companies that offer subscription-based online on-demand streaming of content (such as a library of films and television programs) operate as single-sided providers, and 'do not mediate to enable distinct user types to interact with each other directly'.[49] Indeed, in the economic literature, single-sided entities – which do not benefit from typical platform-

[43] See OECD (2019). An Introduction to Online Platforms., p. 20.

[44] See ibid.: an OPs serve 'at least two different sets of users simultaneously, bringing them together and enabling interactions between them that can benefit the users as well as the platform itself'. Also see Evans and Schmalensee (2016). Matchmakers.: 'Matchmakers are called multisided platforms because they usually operate a physical or virtual place that helps the different types of customers get together'. Similarly see SWD(2016) 172 final., pp. 2-3.

[45] See Armstrong (2006). 'Competition in two-sided markets.' The RAND Journal of Economics **37**(3): 668-691.; Evans and Schmalensee (2008). Markets with Two-Sided Platforms. Issues in Competition Law and Policy (ABA Section of Antitrust Law). **1**.; Evans and Schmalensee (2016). Matchmakers.; Filistrucchi, Geradin, Damme and Affeldt (2013). 'Market Definition in Two-Sided Markets: Theory and Practice.' Journal of Competition Law and Economics **10**.

[46] See Rochet and Tirole (2006). 'Two-sided markets: a progress report.' The RAND Journal of Economics **37**(3): 645-667.

[47] See SWD(2016) 172 final., p. 3.

[48] See De Steel and Larouche (2016). An Integrated Regulatory Framework for Digital Networks and Services. A CERRE Policy Report Brussels, CERRE. , pp. 41-42.

[49] van Eijk, Fahy, van Til, Nooren, Stokking and Gelevert (2015). Digital platforms., p. 13. Matchmakers are called multisided platforms because they usually 'operate a physical or virtual place that helps the different types of customers get together'. See Evans and Schmalensee (2016). Matchmakers. Kindle file.

associated features, such as network effects – are often not considered platforms, but rather as re-sellers, or vertically integrated companies (VIC), depending on whether the content is produced in-house or rather its use has been licenced by third-party producers.

Distinguishing pure resellers and VIC from entities who merely offer a virtual space for interaction – e.g. transactions between suppliers and users of digital content – may indeed be relevant for policy purposes, as the entities' control over the interaction changes significantly according to the business model adopted. By purchasing the inputs from suppliers, resellers decide the price, as well as the conditions for contracting with end-users, and assume most of the commercial risks. Overall, if considered in their 'ideal type', resellers hold full control over the two distinct transactions.

Nevertheless, this distinction shall not lead to cut one-sided platforms out of the picture. Firstly, the level of control exercised over the interactions carried out by the users – despite radically different in their 'ideal-types' – varies significantly in both the business models. In this sense, that of intermediaries and resellers/VIC shall be seen as the extremes of the same spectrum, rather than two radically alternative solutions, with several business models that fall in a grey zone, depending on the level of control exercised on the overall operations.[50]

Secondly, a digital platform *is* or *can* be operated as a two- or multi-sided platform, *but the operator of the platform may choose not to do so*.[51] Platforms may choose to act as pure resellers or distributors, as a multi-sided-platform, or both, according to business strategies that may change over time.[52] Indeed, many companies adopt a hybrid solution, working as intermediaries in some cases as well as re-sellers or VIC in others, so that it may prove difficult to use this as a discriminating criterion.[53] Finally, and most importantly, entities such as on-demand video content providers operating primarily on a single-sided market still give rise to economic, legal and social implications which are common to those displayed by (properly intended) OPs.[54]

This necessarily calls for a revision of the traditional idea of OPs as intermediaries. Indeed, platforms have typically been said to facilitate transactions, exchanges and connections that – had it not provided a virtual space to interact – would have happened at a much higher (transaction) cost or would not have happened at all.[55] It is, therefore, preferable to adopt a broad interpretation encompassing cases in which the operator facilitates the connection between distinct groups, without necessarily allowing direct interaction between them.[56]

Against this backdrop, and for the sake of developing a functional classification of OPs that could help to map their rights, duties and liabilities, the requirement under point (iii) shall be understood broadly,

[50] Thus, the actual level of control exercised by the platform on its users (broadly intended), shall rather be seen as a variable for their analysis – i.e. and element to include in the creation of their classification – rather that a defining element upon which to draw the boundaries of the concept. See § 4.3.

[51] See Batura, van Gorp and Larouche (2015). Online Platforms and the EU Digital Single Market. A response to the call for evidence by the House of Lord's internal market sub-committee Rotterdam. , p. 2.

[52] Similarly see Hagiu and Wright (2014). 'Marketplace or Reseller?' Management Science **61**(1).

[53] On many large online marketplaces the sale of goods is made by the vertically integrated platform operator, as well as by third-party sellers. In this case, the platforms are operated by a company which is also a merchant, while in other cases the platform only operates as an intermediary through its marketplace, where only third-party sellers are active in the transactions as traders.

[54] See SWD(2016) 172 final., pp. 2-3.

[55] Similarly see Rochet and Tirole (2006). Two-sided markets.

[56] Contrary see Hagiu and Wright (2015). 'Multi-Sided Platforms.' International Journal of Industrial Organization **43**: 162-174. where the element of 'direct interactions between sellers and buyers or between two or more distinct sides' is explicitly included as a OPs' qualifying features, precisely to better demarcate their asserted radical difference from resellers and integrated firms.

as to include entities primarily or exclusively offering products and services acquired by third-parties or produced by VIC, whenever this operation still constitutes *overall facilitation of the interaction of the different sides of the market, despite the lack of direct interaction among them*.

On the broad interpretation of the notion of 'service or […] structure offered to other subjects for use' and the need to overcome it. Conversely, defining OPs as the entities offering a digital service or a structure that allows or facilitates interaction among two or more users might prove over-inclusive, leading to extend the study to entities such as Internet Service Providers (ISPs)/ Internet Access Providers (IAPs), i.e., providers of fundamental communications services such as access, information storage, or data connection allowing access to the internet through physical transport infrastructure.[57]

ISPs are often portrayed as 'two-sided platforms',[58] and as belonging to the broad category of 'Information Society Service Provider[s] (ISSPs) and telecoms networks and services',[59] which is sometimes understood as a subcategory of OPs.[60] Indeed, ISPs operate in a multisided market, since they 'link users to the Internet and, thus, to online content providers' and, in this sense, they appear as 'digital service[s] that facilitate interactions between two or more distinct but interdependent sets of users […] who interact through the service via the Internet' in at least in one direction.

However, ISPs differ profoundly from ideal-type OPs such as social networks and marketplaces, ultimately leading to different socio-legal-economic concerns.

Not only they should fall outside the province of this study; from an epistemological perspective, the comparison between ISPs and platforms properly understood may prove fundamental to fine-tune the definition of the latter. While ISPs merely enable communication over the Internet to which they allow access, classic OPs provide infrastructures and services that go beyond the mere provision of Internet access and may indeed build upon the digital service offered by ISPs. In other words, platforms stand out because they provide a series of services known as 'over-the-top (OTT)', i.e. provided to end-users over the Internet, independent of the ISP in control or distribution of the service.[61] In this sense, ISPs offer a first layer of interaction – the access to the communication network – whereas OPs offer additional content, operating on top of the latter.

Moreover, the conceptual distinction among OPs, ISPs, and ISSPs is critical in itself. Said notions have been used, often interchangeably – for the last 20 years when referring to providers of services or

[57] See Perset (2010). The Economic and Social Role of Internet Intermediaries., p.11. Similarly, Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ L 310, 26.11.2015, defines IAPs under Art. 2 as providers of internet access services, i.e. publicly available electronic communications services that provide connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used. Also, the ECD refers to IAPs in Art. 12 as 'information society service providers that provide services consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network'. IAPs liability as mere conduits under Art. 12 and Art. 15 of the ECD was analysed by the CJEU in C-484/14, Tobias McFadden v Sony Music Entertainment Germany GmbH,EU: C:2016:689. As seen in this case, wi-fi network providers are one type of intermediary, that of mere conduits and not hosting providers.

[58] Similarly see Evans and Schmalensee (2016). Matchmakers., Kindle file. 'Matchmakers are called multisided platforms because they usually operate a physical or virtual place that helps the different types of customers get together'.

[59] See Savin (2018). 'Regulating Internet Platforms in the EU: The Emergence of the 'Level playing Field'.' Computer Law & Security Review 34(6): 1215-1231.

[60] As per Recital 17 of the ECD: 'this definition covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression)'. Thus, not-for-profit scientific or educational repositories as well as not-for-profit online encyclopaedias would normally fall outside the definition.

[61] See BEREC (2018). BEREC report on the impact of premium content on ECS markets and the effect of devices on the open use of the Internet., p. 24 ff.

content on the Internet, even when talking about the same business model, as well as to indicate some role or activity assumed by OPs. This may give rise not only to semantic difficulties but also difficulties in understanding the object of regulation and analysis.[62] Indeed, the notion of ISSPs has no real descriptive meaning as it was only created as a legal definition encompassing different objects of regulation. In particular, it was used to define the application of some regulatory frameworks – i.e. Article 12 and 14 ECD – but it overlaps with and includes that of ISP,[63] in so far as it covers services consisting in the provision of basic connectivity services and OTT services. Although these notions may in some cases overlap, they are not identical with respect to their sphere of application, and thus, at least for the sake of this study, they shall be kept separate.

To conclude, for the purpose of defining the object of the study and developing a functional definition and classification of OPs that could help to map their rights and duties, as well as the liability regimes applicable to them, *the requirement under point (i) shall be understood narrowly, as to include only entities offering (primarily) OTT digital services or infrastructures to end-users*. Since ISPs/IAPs do not offer OTT services – and thus do not share the same economic, social and regulatory implications connected to the type of infrastructure and activities enabled over the internet – they fall outside this study's understanding of platforms, and thus will not be directly analysed herein.[64]

Against this background, this study suggests the following tentative definition which could serve as a conceptual tool for identifying and analysing the phenomenon:

> OPs are entities which: (i) offer (primarily) OTT digital services or infrastructures to users, (ii) are or can be operated as a two- or multi-sided market business model, but may choose not to do so, and (iii) allow the overall facilitation of interaction of the different sides of the market, even when there is no direct interaction among them.

4.3 Mapping platforms: a proposed classification

Definitions and taxonomies shall be functionally constructed, i.e. elaborated as to adequately cover technological solutions and business practices based on their social, economic and ethical implications. Furthermore, to be adequate to the specific problem, they shall be narrow-tailored enough to allow legislation that touches upon the relevant and meaningful aspects, while being aware that regulation also needs constant adaptation, despite not at the identical pace of technological advancement.

A platform offering e-commerce services may also give rise to different issues, and ultimately different risks, from those brought about by a search engine or a social network. When regulatory interventions are considered, the characteristic of a specific type of platform, or cluster of platforms are of paramount importance, as well as the various problems associated thereto. This means, however, that not all the categories into which a platform may be classified are relevant for addressing a specific problem.

[62] See Savin (2018). Regulating Internet Platforms in the EU.

[63] See Obergfell and Thamer (2017). (Non-)regulation of online platforms., p. 436.

[64] In a similar vein Directive (EU) 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, PE/26/2019/REV/1, OJ L 136, 22.5.2019, p. 1–27, limits its scope of application to provision of digital services, leaving internet access services outside the its scope. See Recital 19: 'As there are numerous ways for digital content or digital services to be supplied, such as transmission on a tangible medium, downloading by consumers on their devices, web-streaming, allowing access to storage capabilities of digital content or access to the use of social media, this Directive should apply independently of the medium used for the transmission of, or for giving access to, the digital content or digital service. *However, this Directive should not apply to internet access services*' (emphasis added).

Indeed, just as there is no one-size-fits-all definition of 'online platform', multiple taxonomies may be proposed by referring to different features that, to some extent, do overlap.

The proposed classification is specifically designed to sort out those features and types of platforms that are of greater relevance to carry out the requested legal analysis.[65] The availability and simultaneous use of many sorting mechanisms could then enable a compartmentalisation of OPs, giving a more accurate and detailed view of platforms' traits, similarities and differences, essential for accurate policy recommendations.[66] Indeed, the same platform may fall within different strands, because of the multiple services offered.

For this purpose, in section 4.3.1 the study will classify OPs according to a series of relevant criteria: services performed/enabled by the platform, sectors of relevance, actors involved in their functioning, use that OPs make of the data collected through their infrastructure, sources of revenue, level of platforms' control on users' activities.

4.3.1 Criteria: activities, sectors of relevance, actors, use of data, sources of revenue, level of control on users' activities

Activities/Digital services. The first parameter to be used when mapping OPs revolves around the activities performed and the service offered i.e. what they do, and what they allow users to do.[67]

Again, this categorisation can be done according to various levels of specificity, and different studies have presented concurrent taxonomies, varying both for their overall granularity and for the criteria used for compartmentalisation.[68] For the sake of this study, we can distinguish between:

- *Web hosting providers*, allowing users to host a website or other internet-based offering;
- Search engines, allowing users to carry out systematic web searches for particular information specified in a textual web search query, indexing results accordingly;
- *Social media, networking and discussion forums*, allowing users to connect and communicate publicly or semi-publicly;
- *Online media sharing providers*, allowing publication and consumption of online content and which, according to the type of material shared, can be further distinguished in news aggregation and broadcasting, music streaming, video streaming, blogs, etc.;
- *Messaging platforms*, allowing users to communicate and share content privately;
- *Matchmaking and e-commerce platforms*, facilitating the transaction of goods and services, such as marketplaces, app stores, and platforms offering services on long-distance carpooling, labour freelancing/crowdsourcing, travel booking, crowdfunding etc.; within this group, a narrower category may be identified, namely:
- *Collaborative platforms*, offering non-professional actors to offer offline-services on an occasional basis (e.g. short term let of one apartment);
- *Other matchmaking platforms*, such as dating apps;

[65] In the same line, OECD (2019). An Introduction to Online Platforms, pp. 60 ff.

[66] See ibid., pp. 60-61: 'the use of so many sorting mechanisms at the same time enables a right compartmentalisation of online platforms, giving policy makers a more accurate and detailed view of platforms' traits, similarities and difference. […] The most obvious way to construct a typology is on a functional basis. That is to say, the platforms can be sorted based on categories that describe what the platforms do or how they do it'.

[67] Similarly see COM(2016) 288 final, p. 5. European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI)), para. 6-8.

[68] See, e.g.: van Hoboken, Quintais, Poort and van Eijk (2018). Hosting Intermediary Services and Illegal Content Online. An analysis of the scope of article 14 ECD in light of developments in the online service landscape Luxembourg, DG Communication Networks. , p. 13. The study represents the major source of inspiration for the classification here elaborated.

- *File storage and sharing providers*, allowing storage and sharing of digital content online;
- *Online advertising platforms*, allowing websites to host advertisements, and advertisers to run ads on those sites.

If these activities and services can be distinguished in theory, they are not mutually exclusive. On the contrary, platform operators often deliver a mix of them: search engines, for example, also offer a digital infrastructure to advertisers who pay to have a top-display-position within the results of a given search query and thus work as advertisement networks.

Sector of relevance. OPs provide services in several sectors and providing a complete picture of the latter would go beyond the purpose of this analysis. However, a few significant examples can be identified.

One sector where OPs have proliferated is that of financial services (e.g. currency exchange, crowdfunding, mobile payments, online brokers), also known as Fintech, with many OPs offering digital payment services as well as payment intermediation services, including data analytics, risk management, conversion rate enhancement, etc. Moreover, OPs sometime offer financial or payment services, in addition to their main, non-financial related activities. This happens, for example, in the case of social media outlets and online marketplaces that offer payment intermediation services, possibly giving rise to regulatory and supervising concerns. In these cases, the OP is not acting in any manner as an intermediary but as the professional provider of services and goods to its customers (see 'actors' and 'level of control', below), and the rules enacted for the sector-specific services should be equally applicable to OPs providing these services. For example, an OP offering payment intermediation services, may be required to comply with the applicable legislation on financial licenses and authorisations.[69]

Other sectors of relevance where OPs offer specific services are those of transportation,[70] accommodation,[71] food and medicine delivery.[72]

In all these cases, the sector in which OPs operate constitutes another fundamental layer of classification, as it substantially shapes the rights, duties and liabilities which both OPs and their users may be required to comply with.

Indeed, one particular issue which arose in the context of the so-called collaborative economy is whether OPs may be considered as providers of the 'underlying' service contract concluded through the platforms, which, strictly speaking, is delivered on a peer-to-peer basis. Indeed, in its *Uber* and *Airbnb* judgements, the CJEU stated that, to understand whether the OPs qualify as information society service providers, or rather as actual providers of the underlying service (for which specific requirements for market access may be set) it is necessary to consider, on a case by case basis, whether the digital interconnection is economically independent or rather exerts a 'pervasive influence' on the conditions under which the 'offline service' is provided.[73]

---

[69] See Expert Group on Regulatory Obstacles to Financial Innovation (2019). 30 Recommendations on Regulation, Innovation and Finance. Final Report to the European Commission Brussels.

[70] See CJEU, Judgment of 20 December 2017, Case C-434/15, Asociación Profesional Elite Taxi v Uber Systems Spain SL, EU:C:2017:981.

[71] See CJEU, Judgment of 19 December 2019, Case C-390/18, Airbnb Ireland, EU:C:2019:1112.

[72] See Art. 85c of Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products, OJ L 174, 1.7.2011, p. 74–87.

[73] See n. 78 and 79 above.

Actors. As already clarified, OPs create digital environments where different users operate. The number and types of user involved, as well as the activities they engage into, changes substantially depending on the platform involved and the services offered. However, since the fight against illegal/harmful content or behaviour online is 'a problem of many hands',[74] having a clear picture of the actors involved in a platform's operation is of fundamental importance. Said subjects are:

- *Online platform*. The platform enables the interaction between the demand and supply sides of the market through its platform/digital infrastructure. The role actually performed by each online platform changes substantially. In the majority of cases, they act as intermediaries, offering the digital environment to enable the exchange: they may do so without actually engaging in any management, organisation or control of the interactions occurring on it, or play a more active role, for example, indexing the content uploaded by users. Indeed, the level of control exercised by the platform over the content/activities carried out through them is particularly important for regulatory purpose and, thus, it is considered as an autonomous criterion of classification (see 'level of control', below). However, in certain conditions, OPs do not qualify as intermediaries, but as actual providers of the digital services,[75] enjoying significant power in determining the terms under which the professional services will be provided.
- *Platform users*. The OPs' users can be both professionals, consumers and public entities, leading to different kind of interactions, such as B2B, B2C, C2C (peer-to-peer), B2G (business to government) or C2G (consumer to government). For the purpose of this analysis, it is important to distinguish between C2C frameworks, where the users act as both providers (prosumers) and consumers of goods (e.g. second-hand/used products) and/or services (e.g. accommodation, transportation, consultancy), and B2C frameworks, where businesses are enabled to sell their products and/or service to consumers (e.g. online marketplaces). Under the B2B frameworks, businesses transact with each other (e.g. platforms that connect wholesale suppliers with distributors).
- *Economically interested third parties*. The involved participants/users may also include governments and scientists acting either as buyers or suppliers, and, in some cases – such as those fostering the development of software and other applications – groups, coordinating efforts and sharing knowledge ('open innovation').76 In addition, users are also the OPs' customers which benefit from the OPs' performance of different digital services in exchange for fees or data.[77]
- *Advertisers/targeters*. Advertisers or targeters are natural or legal persons that use OPs, such as social media platforms, to algorithmically direct specific messages (advertisements) at a set of users.[78] Advertisers pay the OPs to match and deliver the advertisements with the specific targeted groups, based on given parameters or criteria. The targeted groups are created by the OPs based on profiling techniques based on users' provided, observed, or inferred data.[79] Given the importance of data-based advertising in the digital economy, data brokers and data

[74] Helbergera, N., T. Poellc and J. Piersonb (2018). 'Governing online platforms: From contested to cooperative responsibility.' The Information Society 34(1): 1-14.

[75] Case C-434/15 Asociación Profesional Elite Taxi v Uber Systems Spain, SL EU:C:2017:981.

[76] See Heerschap, Pouw and Atmé (2018). Measuring online platforms, CBS. p. 12.

[77] In any case, the user category is very elastic, and it can be broadly or narrowly constructed. Different user groups can be identified such as: 'advertisers, buyers, sellers, content consumers, content producers, app developers, app users, employers, workers, drivers, riders, hosts, guests, payers, payees'. See OECD (2019). An Introduction to Online Platforms., p. 65.

[78] See European Data Protection Board (2020). Guidelines 8/2020 on the targeting of social media users. Version 1.0., p. 9.

[79] See ibid., p. 12.

analytics companies emerged as a new collateral business model.80 These actors capitalise on advertisers' demand for targeted advertisements and they collect data by means of tracking technologies or they purchase data from different sources, which is then sold in an aggregate form either to OPs or to advertisers or data analytics companies. Sometimes data brokers combine and process the data themselves, instead of selling it to data analytics companies and thus offer a one-stop-shop for the selling and purchase of group profiles.

- *Collaterally affected third-parties*. The last category is comprised of natural or legal persons that are not users of the platform, nor advertisers, but are nonetheless impacted by the OPs' and users' activities. This is the case of intellectual property rights holders, whose rights and legitimate interests may be infringed through the sharing and hosting of illegal online content. Similarly, non-users may be harmed by the actions of OPs' users, whenever harmful content related to the non-users is shared and hosted on the platform. Under this category, we can also include the business users that do not have a contractual relationship with a search engine type of platform, since their websites are crawled, indexed, tagged without the knowledge or active participation of the business.[81]

Use of data. In the digital platform economy, OPs' business models and sources of revenue are closely interlinked with data monetisation strategies, and the use of data.[82] Thus, analysing how OPs capitalise on data is an important aspect of government intervention and regulation, and relevant to its effectiveness.

Data may be used in different ways and for different purposes.[83] Based on the role that data have for the platforms' core function within each business model, we can distinguish between:[84]

- *Data-enabled OPs:* platforms that 'have developed revenue generation strategies fully reliant on data and that would not exist without access to large amounts of data and advanced data analytics'.[85] This is the case of social media platforms, networking platforms and online marketplaces where data is used both (i) to provide their services of matching the users and/or the demand and supply sides of the market, and (ii) to provide advertisement services. Furthermore, revenue might also be generated by selling or licensing data or selling new data-related products.[86]
- *Data enhanced OPs*: platforms that use data-generated information to enhance or improve their operations, existing products, or efficiency.[87] In said cases, data do not represent their core

[80] See ibid., p. 9.

[81] See European Commission (2018). Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services. SWD(2018) 138 final Brussels, European Commission. , p. 7.

[82] See Nguyen and Paczos (2020). Measuring the Economic Value of Data and Cross-Border Data Flows. A Business Perspective, OECD. , p. 9.

[83] E.g. data may be used for: 'optimising the platform website, providing a better user experience, advertising, other business purposes, operating, maintaining and providing the features and functionality of the platforms' products and services, communicating with their users, measuring traffic and usage trends, understanding more about the demographics of their users, providing personalised content and information, including targeted content and advertising, diagnosing or fixing technology problems, suggesting local events to attend, serving location-based ads, conducting audits, safety and security, attracting users and increasing their use of the platform, developing new services'. See OECD (2019). An Introduction to Online Platforms., 67.

[84] See Nguyen and Paczos (2020). Measuring the Economic Value of Data., p. 5.

[85] See ibid., p. 10.

[86] See ibid., p. 5.

[87] See ibid., p. 5.

business model and it is instead used for product or service development, predicting demand or identifying cross-selling opportunities.[88] In the platforms' ecosystem, these types of business models are not the rule, but the exception. Their source of revenue is usually based on users' subscription fees.

It shall be taken into account that certain business models, may shift in the future to a data-enabled business model, due to relevant data collection and accumulation.

Data-centred business models and revenues incentivise behaviour that could harm consumers' welfare on many strains. First, the incentives for compliance with data protection rules and practices are lower for data-enabled OPs, than for platforms based on data-enhanced business models. Second, the incentives to retain profits derived from data ownership and processing may be higher than the incentives to share it and contribute to its free flow, as well as to a European data market. Third, data-enabled platforms accumulate large datasets which can lead to the creation of monopolies or oligopolies, and, fourth, may preclude new entrants from thriving, as they have a competitive advantage in developing new products and services based on the information they possess. Fifth, data-enabled companies can better tailor their existing services, increase their users on both sides of the market, and consequently create lock-in effects on their very users.

Sources of revenue. Understanding the OPs' sources of revenue may help policy makers in analysing incentives for platforms' compliance with extant regulation and assess the need for reform.

Based on the classification of actors, sources of revenue may be divided into:[89]

- *Revenue from the supply side of the market*. Such revenue may consist of subscription fees, such as in the case of storage cloud platforms and data analytics platforms. Also, OPs may charge transaction fees, such as in the case of online marketplaces or auction platforms. Another revenue stream may consist of services fees. For example, OPs may offer optimisation consultancy services or offer educational or professional training. Lastly, OPs such as search engines and online marketplaces may offer preferential placement on the web pages or search results in exchange for a fee.
- *Revenue from the demand side of the market.* Said revenue may consist of subscription fees such as in the case of VIC. Content hosting providers also charge users for an ad-free use of digital services. In this latter case, OPs use users' data to attract advertisers which pay for advertisement services, while users pay for blocking advertisements. Certain OPs also charge transaction fees, such as in the case of online payment services and accommodation platforms.
- *Revenue from the advertisement and the third-party side of the market*. Said revenue is closely related to OPs' use of data. When data is used for advertisement purposes, OPs are paid by advertisers, based on different payment models. Some OPs charge a subscription in exchange for advertisement placement. Often times, advertisers pay: (i) for each time an ad is clicked (pay-per-click), (ii) for each time it is shown (pay-per-impression), (iii) for when it leads to a transaction (pay-per-transaction).[90] Advertisements are often the most important revenue source for OPs and the more users the OPs have, the more attractive the OPs becomes for advertisers.[91] This is usually the case for OPs that rely on a zero-pricing business model, where

[88] See UK Government Office for Science (2020). Evidence and scenarios for global data systems. The Future of Citizen Data Systems United Kingdom. , p. 43. Nguyen and Paczos (2020). Measuring the Economic Value of Data., p. 15.

[89] See van Hoboken, Quintais, Poort and van Eijk (2018). Hosting Intermediary Services and Illegal Content Online, p. 17 ff.

[90] See ibid., p. 18.

[91] See Heerschap, Pouw and Atmé (2018). Measuring online platforms.,p. 10.

no fees are paid by the users in exchange of the OPs digital services, and the main source of revenue is comprised of fees paid by advertisers.

- *Other data-generated revenues*. As previously mentioned, data-enabled OPs benefit from two additional data revenues streams from (i) selling the data to data-brokers and/or (ii) using the data to create new services and products and/or improve existing services, which is also referred to as value-creation.[92]

Level of control on users' activities. As anticipated, the level of control that OPs acting as intermediaries exercise over the content, information and exchange carried out through their infrastructure varies significantly.[93]

- At the one side of the spectrum, OPs acting as mere intermediaries provide no control or governance and users are not restricted in sharing and posting any type of content. This is usually the case with websites hosting illegal or piracy materials, and with forum-type OPs.
- At the medium of the spectrum, there are OPs that engage into activities of management, organisation, and control over the interactions (e.g. indexing) between the sides of the market, to ensure the functionality of the infrastructure, without reaching a full scrutiny over the content and information exchanged. This could also be the case of SMEs which do not have highly advanced filtering technologies (both for showing content based on profiling and for removing it)
- The other side of the spectrum is comprised of large platforms whose business models, policies, guidelines, and terms of service grant them a particularly strong level of control, making them de facto 'regulators' over the activities carried out through their infrastructure. Because of this role, they are often referred to as 'gate-keepers', whose capacity to engage in content-moderation activity – such as monitoring, tracking and removal of information – has significant implications on the respect of fundamental rights and freedoms online, with particular reference to users' data protection and freedom of expression.[94]

[92] See van Hoboken, Quintais, Poort and van Eijk (2018). Hosting Intermediary Services and Illegal Content Online. : 'value creation exists when a service creates potential value that can be turned into revenues (or lump-sum buy-out) at a later stage'.

[93] Similarly, for peer-to-peer transaction platforms see Hausemer, Rzepecka, Dragulin, Vitiello, Rabuel, Nunu, Rodriguez Diaz, Psaila, Fiorentini, Gysen, Meeusen, Quaschning, Dunne, Grinevich, Huber and Baines (2017). Exploratory study of consumer issues in online peer-to-peer platform markets Brussels, Consumers. , p. 56 where the authors identify three types of business models, depending on the level of control, namely: (i) Hosting of listings platforms; (ii) Actively managed transactions type of platforms; and (iii) Platform governs transactions.

[94] See Access Now, ARTICLE 19, COMMUNIA association, Centrum Cyfrowe, Civil Liberties Union for Europe, Civil Rights Defenders, Creative Commons, dataskydd.net, Electronic Frontier Foundation, European Digital Rights (EDRi), Global Forum for Media Development, Homo Digitalis, Idec - Brazilian Institute of Consumer Defense, Open Knowledge Foundation, OSEPI, Panoptykon Foundation, Privacy International, Ranking Digital Rights, Rights International Spain and Xnet (2020). Joint statement in response to the inception impact assessments on a new competition tool ex ante regulatory instrument for large online platforms acting as gatekeepers Brussels.

Table 3 - OPs' Classification

OPs' Classification	
Activities	➢ Web-hosting providers ➢ Search engines ➢ Social media, networking and discussion forums ➢ Online media sharing providers ➢ Messaging platforms ➢ Matchmaking and transaction e-commerce platforms (subcategory: collaborative platforms) ➢ Other matchmaking platforms ➢ File storage and sharing providers ➢ Online advertising platforms
Sector of relevance	➢ e-Commerce ➢ Fintech ➢ Transport ➢ Accommodation ➢ Personal services ➢ Advertising ➢ News and media ➢ Electronic communication ➢ Health care ➢ Etc.
Use of data	➢ Data-enabled OPs ➢ Data-enhanced OPs
Actors	➢ OPs ➢ Users ➢ Advertisers/Targeters ➢ Economically interested third-parties ➢ Collaterally affected third-parties
Sources of revenues	➢ Revenue from the supply side of the market ➢ Revenue from the demand side of the market: subscription fees; users' ad-free use fee; transaction fees ➢ Revenue from the advertisement and third-party side of the market: subscription fees for advertisement placement; pay-per-click fees, pay-per-impression; pay-per-transaction ➢ Other data-generated revenue: selling the data to data brokers and/or; using the data to create new services and products and/or improve existing services, which is also referred to as value-creation
Level of control	➢ Low-level of control ➢ Medium-level of control ➢ High-level of control

5. Liability of online platforms

This second section of the study is devoted to the description, evaluation and assessment of the liability regimes that come into play when illegal /harmful material – content or product – is made available on OPs' infrastructure. In particular, it discusses the current distribution of rights, duties and sources of liabilities (as well as the associated remedies) among the different actors involved, with specific reference to: the different types of infringement; the different types of OPs involved, relying on the classification proposed in Chapter 4; the different types of users and third parties involved, again, in light of the above-referred classification.

In the mapping of the whole range of liability, the study will identify and describe the EU regulatory framework applicable to each type of infringement/societal concern, considering both hard law and soft law, as well as the voluntary measures adopted by online platforms to address liability, if any. Reference to national and international law is also made, whenever relevant (Chapter 6).

In doing so, the study will distinguish between OPs' liability connected to the activities performed or the content uploaded by its users (§section 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8) and alternative sources of liability, such as contractual liability against both its business users and consumer-users, as well as liability deriving from infringements of privacy and data protection law (§section 6.9-6.10). Indeed, even if said framework does not deal with the illegality/harmful nature of the material uploaded on the platforms itself, but rather on the activities performed by the platforms, having a broad understanding of the legal position of platforms in the major fields of law is fundamental to adequately assess the regulatory challenges associated with their operation, as well as their incentives to combat illegal activities carried out through the infrastructures and services they offer.

For each type of liability, the study reviews the main legal/regulatory challenges associated with the operation of OPs and analyses the incentives that the different subjects involved have to prevent, detect, remove and remedy for the upload of illegal and/or harmful material, depending on the specificity of the case.

These two steps will offer the basis for the policy proposals under Chapter 8 below.

5.1 Types and functions of liability rules

Setting the conceptual framework. (i) Difference between responsibility and liability. Responsibility, as typically referred to in the law and policy debate revolving around advanced technologies, is a wider concept than that of liability, and it is often used to denote the *moral* responsibility of a subject, as defined by the philosophical, sociological or political debate.

On the contrary, liability denotes that specific form of *legal* responsibility that is connected to the violation of a duty that the person held liable was obliged to comply with, or to the infringement of one's rights. Liability rules, indeed, shape the legal position of OPs, and contribute in determining their incentives toward the prevention, removal and remedy for the upload of illegal/harmful content. Nevertheless, the emerging pictures and the connected incentives vary significantly depending on the type of liability involved.

In the policy-making debate, sometimes the distinction between responsibility and liability is blurred. In this sense, it is commonly said that OPs are 'responsible for' obtaining a certain desired goal, because they are deemed as bearing the moral and social responsibility, e.g., of addressing the socio-economic effect deriving from their activity, or because they are believed to be in the best position to do so, in response to the 'gatekeeper role' they assumed over the years. Indeed, the discussion on the need to

make them 'accountable' often passes through the discussion on their liability for the illegal/harmful content they host.[95] However, the two profiles should be kept separated. Claiming that OPs should be responsible for ensuring a certain online environment does not necessarily mean that they have or should have a legal responsibility to do it, and – even if that happened to be the case – it does not clarify what type of liability is or should be imposed.

(ii) Differences between administrative, criminal and civil liability. Rationales and structure of civil liability. Indeed, liability may be criminal, administrative or civil.

In criminal matters, liability arises because of a court decision, when the prosecutor demonstrates beyond a reasonable doubt that the defendant's conduct meets both the mental and the material elements required for the offence to be punished under criminal law, and consists in fines and imprisonment, as well as other non-custodial punishments.

Administrative liability is a type of financial responsibility imposed by agents of the public administration, to sanction the infringer and compensate for the wrong caused.

Civil liability, instead, determines who is supposed to bear the negative economic consequences arising from an accident, and under which conditions.[96]Typically, the party is held liable, and thence bound to compensate, that is deemed to have caused the accident, and therefore is responsible for it. Liability is established after a trial, where the claimant, who sued the wrongdoer, has to prove the existence of the specific constitutive elements that ground the liability affirmed.[97]

Civil liability rules pursue two distinct functions, namely: (i) ex ante deterrence, since they aim at making the agent refrain from the harmful behaviour, given that s/he will have to internalise the negative consequences caused; (ii) ex post compensation of the victim, as they force the person responsible for the damage to make good for the loss caused.[98]

Many different theories have been elaborated to justify civil liability, as well as to shape liability rules within a legal system according to specific ideologies; most of them are related to different notions of justice (retributive or corrective),[99] or economic efficiency.[100]

Nowadays, legal systems do not commit to only one theory of tort and justice, but rather to a combination of them: the same normative framework will feature different models of liability rules, displaying a variety of imputation criteria (causation/remoteness, subjective element), which in turn reflect the peculiar rationales underlying the attribution of liability. Many tort law systems have a general rule prescribing liability for damages caused by reprehensible behaviours on the basis of fault. This solution is moved by all the different goals defined above: not only ex post compensation and sanction, but also ex ante deterrence, since fault-based liability incentivises agents to adopt the

[95] See, e.g. the COM(2017) 555 final., p. 2: 'Online platforms which mediate access to content for most internet users carry a significant social responsibility in terms of protecting users and society at large and preventing criminals and other persons involved in infringing activities online from exploiting their services', and thus 'should decisively step up to address this problem, as part of the responsibility which flows from their central role in society', which also covers the need to balance the fight against illegal content and protection of the different fundamental rights at stake.

[96] Similarly, liability means 'the law determining when the victim of an accident is entitled to recover losses from the injurer'. See Shavell (2007). Liability for Accidents. Handbook of Law and Economics. Polinsky and Shavell. Amsterdam, Elsevier**:** 142.

[97] See Van Gerven, Lever and Larouche (2000). 'Tort law of Entry.' Tort law of WebLog 2000.

[98] See Polinsky and Shavell (2009-2010). 'The uneasy case for product liability.' Harvard Law Review **123**: 1437-1492., p. 1441.

[99] See Walen (Winter 2016 Edition). Retributive Justice. The Stanford Encyclopedia of Philosophy. Zalta. URL = <https://plato.stanford.edu/archives/win2016/entries/justice-retributive/>.Coleman, Hershovitz and Mendlow (Winter 2015). Theories of the Common Law of Tortsibid. https://plato.stanford.edu/archives/win2015/entries/tort-theories/.

[100] See Calabresi and Melamed (1972). 'Property Rules, Liability Rules, and Inalienability: One View of the Cathedral.' Harvard Law Review 85(6): 1089.

standard of care necessary to avoid harmful behaviours, as to avoid the negative economic consequences deriving from the duty to compensate[101]. Sometimes, however, the defendant is held liable merely because of the particular position that s/he held towards the cause of the damage, e.g. because of the economic or otherwise benefit associated with possessing or running a dangerous product or activity. This model is often associated to a strict or semi-strict liability basis, depending on whether or not the defendant may exclude his duty to compensate – i.e. by demonstrating that he took all the necessary measures to prevent the harm to occur, or by demonstrating that the latter was caused by an act of good –. The stricter the liability, the more compensation-oriented, instead of deterrence- and punishment-oriented the rationale.

Further down this line, sometimes liability is ascribed to the person who is best positioned to manage and internalise the risk, preventing its occurrence and minimising its consequences, as well as to compensate the victim once an accident occurs. Such model is particularly common in Law and Economics literature.[102] A peculiar version of this model is the so called risk management approach (RMA), which is grounded on the idea that liability should not be attributed on the basis of considerations of fault – defined as the deviation from a desired conduct – typical of most tort law systems, but rather on the party that is best positioned to (i) minimise risks and (ii) acquire insurance. It moves from the basic consideration that – despite liability rules may well work as incentives or disincentives towards specific behaviours – they may not ensure sufficient and efficient incentives towards a desirable ex ante conduct, be it a safety investment – e.g. in the case of producers' liability – or a diligent conduct – e.g. in the case of road circulation –, and that end is best attained through the adoption of detailed ex ante applicable regulation, such as safety regulation. According to this view, liability rules should thus be freed from the burden of incentivising the agents towards desired conducts, and rather be shaped as to ensure the maximum and most efficient compensation to the victim. In extreme cases, this could also be designed as to avoid the difficulties and burdens connected to traditional judicial adjudication, and rather be based on no-fault compensatory funds.[103]

(iii) Differences between primary liability and secondary liability. Another fundamental distinction is that between primary and secondary liability.

Primary liability refers to an obligation for which a party is directly responsible. Platforms are liable directly in case of failure to comply with duties ascribed directly to them: e.g. the duty to present specific information to its business users under the Regulation(EU) 2019/1150 (also see section 6.9.2).[104]

Secondary liability, on the other hand, refers to an obligation that is the responsibility of another party if the one which is directly responsible fails to satisfy the obligation in the first place. In some case, parties will attempt to attach primary liability to 'secondary' actors. Differently from the previous case, an online platform is liable under a 'secondary or intermediate liability', when it is held responsible for the mere fact that its intermediation enabled the users' illegal and harmful activities. Under EU law, there is a harmonised conditional exemption for this type of liability for hosting providers under the ECD (Article 14-15, see §6.1). However, in as much as Member States may impose on platforms a duty of care relating to the content, materials and services provided by its users over the platforms' digital

[101] Polinsky and Shavell (2009-2010). 'The uneasy case for product liability.' Ibid. **123**: 1437-1492.

[102] See Polinsky and Shavell (2007). 'Handbook of Law and Economics of Entry.' Handbook of Law and Economics of WebLog 2007.

[103] See Palmerini and Bertolini (2016). Liability and Risk Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice. Schulze and Staudenmayer. Baden-Baden, Nomos**:** 225-259, Bertolini (2016). 'Insurance and Risk Management for Robotic Devices: Identifying the Problems.' Global Jurist **16**(3): 291-314.

[104] See Regulation (EU) 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, PE/56/2019/REV/1, OJ L 186, 11.7.2019, p. 57–79

environment (without violating the prohibition of a general duty to monitor, under Article 15 ECD), the distinction between primary and secondary liability tends to blur.[105]

(iv) Difference between harmful/illegal online content. Likewise, it is important to differentiate between harmful and illegal content online, 'since the two pose different issues and may call for different legal and technological responses'.[106]

Online illegal content is that violating European and national rules setting what cannot be used, communicated and/or distributed, according to the principle 'what is illegal offline is illegal online'.[107] The qualification of a given material as unlawful may respond to the need of protecting general societal interests and the public order (e.g. in the case of content that incites to terrorism), fundamental personal interests and rights (e.g. in the case of non-legitimate treatment of personal data), or individual economic rights with important social relevance (e.g. distribution of content in breach of exclusive rights under IP law). Depending on the nature and gravity of the content, the unlawfulness will be set solely under civil and administrative law, or also involve criminal liability.

Harmful content, instead, is not considered per se illegal, but its use and consumption are likely to cause some harm to society or – most likely – to particularly vulnerable subjects; thus, its distribution is often allowed, yet subject to specific safeguards. Differently from illegal content, 'merely' harmful content is much harder to define *a priori*.

Despite Member States' regulation differ with respect to both illegal and harmful content, seeking convergence with respect to the latter is certainly more problematic, given the higher bearing of cultural social sensitivity upon it.[108]

6. Applicable framework: identification, analysis and assessment

OPs' liability regime is particularly complex and fragmented, as it consists of

- A baseline regime set in the ECD, which harmonises the negative conditions of secondary liability, thus establishing under which circumstances OPs cannot be held liable under national law;
- A series of sectoral forms of primary liabilities to further shape the duties of specific OPs for given types of activities and against specific types of infringements, deriving from both EU and national laws;
- A series of guidelines and indications on OPs' duties and liabilities set up in soft law and voluntary instruments, such as the ones recalled in Chapter 3 above;
- A series of duties which OPs have agreed upon through self-regulatory measures for specific types of activities and against specific types of infringements.

[105] This distinction is sometimes downplayed when general reference is made to 'intermediaries' liability', intended as the specific type of liability which online intermediaries bear, which – however – is both primary and secondary in kind. On this matter, extensively, Riordan (2020). A Theoretical Taxonomy of Intermediary Liability. Oxford Handbook of Online Intermediary Liability. Frosio. United States of America, Oxford University Press.

[106] See European Commission (1996). Communication from the Commission. Illegal and harmful content on the Internet. COM(96) 487 Final Brussels, European Commission. , p. 10.

[107] See COM(2017) 555 final., p. 2. Also see de Streel, Defreyne, Jacquemin, Ledger, Michel, Innesti, Goubet and Ustowski (2020). Online Platforms' Moderation of Illegal Content Online. Law, Practices and Options for Reform Luxembourg, Policy Department for Economic. , p. 77.

[108] See § 6.5.

6.1 e-Commerce Directive and the platform's intermediary liability

Directive 2000/31/EC on electronic commerce in the EU. (i) Home control principle and liability exemptions. As we have anticipated, OPs may be held liable for the illegality of their users' activities, which took place thanks to the context or infrastructure provided by them. At EU level, the general framework for OPs' liability is to be found in the E-Commerce Directive 2000/31 (ECD).[109] The so called 'e-Commerce Directive' sets standard harmonised rules on various issues related to electronic commerce.[110] Most importantly, it establishes the 'country of origin/home control principle' according to which OPs are subjects to the legal requirements of their Member States of establishment, and it harmonises the conditions under which certain 'information society service providers' – those providing conduit, cashing and hosting of information at the request of third parties – benefit from the exemption of liability for the illegal content hosted by them (so called 'Safe Harbour').[111] In particular:

- Pursuant to Article 12, where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network (*mere conduit*), Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. This also applies in case of automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
- Pursuant to Article 13, where the service offered by the ISSP consists in the transmission in a communication network of information provided by a recipient of the service (*cashing*), Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that the provider (a) does not modify the information; (b) complies with conditions on access to the information; (c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

[109] See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

[110] It covers a broad series of online services: news services (news websites), basic intermediary services – internet access, transmission and hosting of information – etc. etc. Under the ECD, operators providing the aforementioned services are subject to regulation only in the EU country of their registered headquarters (home-control principle). They shall conform to a variety of norms, not all of them relevant for the purpose of this study. Operators are required to publish basic information on their activities (name, address, trade register number etc.) in a permanent and easily accessible form, follow specific rules on advertising and spam. Specific rules on the legal status of electronic contracts, the information to be provided thereof and the placing on online orders are also set, while the adoption of codes of conducts and online out-of-court dispute settlement mechanisms are encouraged.

[111] See Art. 15 of the ECD. Also see Riis and Schwemer (2019). 'Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation.' Journal of Internet Law **22**(7): 1–21., p. 3. Montagnani and Trapova ibid.'New Obligations for Internet Intermediaries in the Digital Single Market - Safe Harbors in Turmoil?': 3-11., p. 3.

- Pursuant to Article 14, when the providers' service consists of the storage of information provided by a recipient of the service – who is not acting under the authority or control of the provider – (*hosting*), Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that the former (a) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

This 'Safe Harbour Regime' is of horizontal and general application, thus excluding intermediaries from a wide range of liabilities – criminal, administrative and civil – for all the activities carried out by third parties through their platforms, provided that the conditions recalled above are met. In this sense, it excludes them from secondary liability, unless a series of duties of care established therein are not complied with (e.g. prompt removal of the information upon knowledge of its illegal nature). However, as indicated below, sectoral legislations have been adopted, which – despite not affecting the regime of secondary liability exclusion just described – complement it with a wide range of additional duties of care, creating parallel regimes of rights and duties depending on the type of infringement involved.

(ii) Distinction between active and passive intermediaries. By relying on recital 42 of the ECD[112], the Court of Justice has further elaborated this regime, stating that only 'passive' intermediaries can benefit from the liability exemption under Article 12-14 ECD.[113] When facing the task of clarifying what makes and entity a passive or an active intermediary, the Court stated providers of mere conduit and caching are more likely to be passive, since by the nature of the service they offer they may have limited or no knowledge of the content conveyed, while a more careful assessment is due for hosting services providers. Here, the Court repeatedly stated that 'as regards a communication network access provider, the service of transmitting information that it supplies is not normally continued over any length of time, so that, after having transmitted the information, it no longer has any control over that information. In those circumstances, a communication network access provider, in contrast to an internet website host, is often not in a position to take action to remove certain information or disable access to it at a later time'.[114]

(iii) Notice and Take Down procedures, prohibition of general monitoring and call for self-regulation. In all these cases, the relevant liability exemption does not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, to require the service provider to terminate or prevent an infringement.

Furthermore, Article 15 states that under national law, ISSPs might hold a duty to promptly inform public authorities of alleged illegal activities undertaken or information provided by recipients of their service, and to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements. However, such

[112] See Recital 42 of the ECD: 'The exemption from liability established in this Directive covers only cases where the activity of the information society service is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that information society service providers has neither the knowledge of not the control over the information which is transmitted or stored'.

[113] Please allow reference to: Cases C-236/08 to C-238/08 Google France v Louis Vuitton EU:C:2010:159, para. 113; Case C-324/09 L'Oreal et al. v. eBay EU:C:2011:474, para. 116; Case C-484/14 Mc Fadden EU:C:2016:689, para. 62.

[114] See Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, Case C-484/14, EU:C:2016:689.

an obligation cannot consist in a general duty to monitor the content of the information transmitted or stored.

Although Member States are prohibited from imposing general obligations to monitor the content made available through the platform, the ECD largely encourages OPs to adopt self-regulatory instruments to tackle detection, removal and disabling access to illegal content.[115]

Soft law. Commission Recommendation on tackling illegal content online. As anticipated in Chapter 3 above, in March 2018 the Commission proposed a series of measures to be adopted by Member States and OPs to ensure quick and proactive detection, removal and prevention of reappearance of illegal content, to be defined according to the 'what is illegal offline is illegal online' principle.[116] Those measures consist of:

- *Clearer 'notice and take down action' procedures* (NTD). OPs were asked to provide easy and transparent rules for notifying illegal content and fast-track procedures for 'trusted flaggers'. At the same time, they were asked to inform content providers and give them the opportunity to contest the action, eventually avoiding the removal of licit content.
- *More efficient tools and proactive technologies*. OPs were asked to provide clear notification systems, as well as proactive tools for the detection and removal of illegal content, in particular in cases of terrorism and child sexual abuse, counterfeited goods and – in general – of content which is potentially highly harmful and does not require contextualisation to qualify as illegal.
- *Stronger safeguards to ensure fundamental rights*. OPs were requested to put in place effective and appropriate safeguards, including human oversight and verification where automated tools and filters are used, to ensure that decisions to remove content are accurate, well-founded and fully respectful of fundamental rights, (freedom of expression, privacy and data protection in particular).
- *Closer cooperation with authorities*. Online platforms were asked to promptly inform law enforcement authorities upon evidence of a serious criminal offence, or reasons to suspect a threat to life or safety of users or third parties, deriving from the illegal content present on their infrastructure or service.
- *Special attention to small companies*. Finally, the recommendation advocated for the adoption of voluntary arrangements, tools for sharing experiences and best practices, as well as technological solutions, including those enabling automatic detection, with the aim of benefitting smaller platforms, which may lack the necessary resources and experiences to adopt a higher degree of governance for tackling illegal content online.

However, and most importantly, the adoption of all these measures was expressly stated as not affecting the liability regime set out in the ECD.[117]

6.1.1 Discussion

The ECD was designed to facilitate online activities, as it strives to set an adequate balance of all the interests at stake: by harmonising liability exemptions, it incentives online intermediation given the social benefits associated with it, while ensuring prompt taking down of illegal content. Indeed, the Commission's public Consultation carried out in 2016 demonstrated a general support for the

[115] See Recital 40 ECD.

[116] See C(2018) 1177 final.

[117] See ibid., para. 24

intermediary liability principles of the ECD, with request for amendment and clarification on specific aspects.[118]

Indeed, it is now widely acknowledged that, as it stands, the ECD, presents a series of critical issues.[119]

Critical issues. (i) Legal fragmentation. Firstly, the ECD has been differently implemented across Member States, with a variety of different judicial interpretations at national level, leaving liability of OPs a largely fragment field. A significant example is represented by the conditions required for platforms to comply with a NTD request, with some Member States specifically calling for courts' orders, and other merely requiring a request from enforcement authorities,[120] whereas some Member States complement these procedures with 'stay down request', obliging intermediaries to ensure that the content is not re-uploaded, or simply allowing intermediaries to discard their duties by forwarding the notification to the alleged infringer, with no further obligations deriving therefrom.

Secondly, conceptual and practical uncertainties remain regarding the very constitutive elements of the regime set out in Article 12-15 ECD.

(ii) Personal scope of application. One major issue concerns the very definition of the entities covered by the directive – intermediaries normally offering services provided for remuneration by electronic means upon an individual request of a user –, and, more precisely, those which can benefit from the exemption under Article 14 ECD. As for the first issue, it is unclear, for example, whether the requirement of a 'service normally provided for remuneration' is met by entities who offer their services for free (an option which, *de facto*, is based upon an implicit qualification of the users' data as 'counter-performance'; see section 4.3.1) or under the 'freemium/premium model', i.e. when the basic service is offered for free, and only additional services or more advanced subscription are subject to payment. As for the second issue, the so called 'Web. 2.0' economy has seen the diffusion of services like cloud computing and storage, online advertising platforms, collaborative platforms and social media – that – while significantly changing the digital ecosystem – raise the question of their potential liability for third party unlawful activities.[121]

(iii) Distinction between 'active' and 'passive' intermediaries. Most importantly, a substantial uncertainty affects the actual meaning of the active/passive distinction, and the extent to which activities such as ranking, indexing, provision of review systems, etc. suffice to elevate the platforms' management of the infrastructure and the content hosted as actual control, and thus waving the liability exemption under Article 14 of the ECD.

(***iv) Effect of proactive measures.*** Likewise, despite OPs are constantly called – even by the ECD itself – to step up in the fight of illegal/harmful content, e.g. by means of voluntary and self-regulatory

[118] See European Commission (2017). Final report on the E-commerce Sector Inquiry. COM(2017) 229 final Brussels, European Commission. ; European Commission (2016). Commission Staff Working Document. Preliminary Report on the E-commerce Sector Inquiry. SWD(2016) 312 final Brussels, European Commission.

[119] Sartor (2017). Providers Liability: From the eCommerce Directive to the future. In-Depth Analysis for the IMCO Committee Brussels, Policy. , De Steel and Larouche (2016). An Integrated Regulatory Framework for Digital Networks and Services. de Streel, Defreyne, Jacquemin, Ledger, Michel, Innesti, Goubet and Ustowski (2020). Online Platforms' Moderation of Illegal Content Online., Schulte-Nolke, Ruffer, Nobrega and Wieworowska-Domagalska (2020). 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 Luxembourg, Policy Department for Economic, Lomba and Evas (2020). Digital Services Act. European added value assessment Brussels, Service.

[120] See Lomba and Evas (2020). Digital Services Act. European added value assessment, De Steel and Larouche (2016). An Integrated Regulatory Framework for Digital Networks and Services., p. 13.; European Commission (2017). Commission Staff Working Document on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for All. SWD(2017) 155 final Brussels, European Commission.

[121] See van Hoboken, Quintais, Poort and van Eijk (2018). Hosting Intermediary Services and Illegal Content Online., p. 8.

means, it is unclear to what extent the adoption of pro-active measures may turn against the interest of the platforms, in as much as it could possibly lead to qualify them as 'active' platforms, and, thus, to lose the liability exemption which they could benefit from in the first place.

(v) Threshold of knowledge justifying the exemption. Similarly, serious uncertainties remain over: (i) what constitutes an 'illegal content or activity' – whether or not it also includes harmful material, and whether essentially contestable qualifications, e.g. over content possibly constituting defamation or disinformation can automatically trigger the intermediaries' duty of removal –, (ii) what constitutes 'actual knowledge' or 'awareness' – if a specific court order or notice is required, or if general awareness would suffice –,[122] as well as over (iii) what timeframe can be said to ensure an 'expeditious' reaction to the infringement. Absent a clarification from the CJEU, all these elements are subject to different implementation or understanding at national level.

(vi) Distinction between general and specific monitoring obligations. Last but not least, the distinction between 'specific content monitoring obligations' and 'general duty of care' is often blurred: obligations to take down and stay down – if broadly framed – require OPs to engage into a constant monitoring, which may not only constitute a substantial violation of Article 15 ECD, but also pose a series risk of over-monitoring and over-removal.[123] Indeed, the issue seems to suffer from a regulatory gap, as no procedural safeguards are set by the ECD.

Uncertainties leading to suboptimal level of content-management. Most importantly, all these issues negatively affect the incentives towards an optimal level of control over online content. In as much as they lead to legal uncertainties, they lead to higher transaction and litigation costs, without having a positive effect on OPs' engagement in fighting online illegal/harmful content. In particular, the uncertainty over the effect of pro-active measures over the qualification of a platform as 'active', and on the 'knowledge' on the presence of illegal content on the platform, substantially reduce OPs' incentives to step up in any time to moderate content, as it may result in losing the liability exception (also known as the 'Good-Samaritan Paradox').[124] At the same time, whenever pro-active monitoring activities are indeed implemented – especially when connected to specific types of infringements (see section 6.2 and 6.3 below) – the risks of automated filtering leading to Type II error and a general tendency toward over-enforcement may constitute a dangerous violation of users' rights, especially as far as the right to information and freedom of speech are concerned.

Policy making and academic debate. Furthermore, the platform operators' contractual freedom and ability to be shielded from liability has been criticised as outdated and at risk of creating a serious

[122] According to the CJEU in Case C-324/09 L'Oreal et al. v. eBay EU:C:2011:474, para. 120, the exemption of liability as under Article 14 of the E-Commerce Directive requires that an intermediary should not have been aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question. Also see Madiega (2020). Reform of the EU liability regime for online intermediaries. Background on the forthcoming digital services act Brussels, European Parliamentary Research Service. , p. 6 and Brunner (2016). 'The Liability of an Online Intermediary for Third Party Content. The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia.' Human Rights Law Review **16**(1): 163–174.

[123] Indeed, in Case Scarlet v Sabam C-70/10 EU:C:2011:771 and Case C-360/10 Sabam v Netlog EU:C:2012:85 the Court claimed that Member States could not impose and internet service provider or a social network to install filtering systems to prevent copyright infringement, precisely because this would be contrary to Art. 15 E-Commerce Directive. However, it also stated that narrower filtering obligations are not precluded but did not to clarify the boundaries between the two. On a similar matter concerning defamatory content on social network in case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited EU:C:2019:821 the CJEU stated that Facebook Ireland could be ordered to find and delete comments 'identical' and 'equivalent' to an illegal defamatory one, thus substantially leading towards a very broad content-monitoring obligation. Also see Kohl (2013). 'Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2).' International Journal of Law and Information Technology **21**(2): 187-234.

[124] See Lomba and Evas (2020). Digital Services Act. European added value assessment, p. 289.

'liability gap',[125] leading to a call for regulatory intervention which could protect platform users and ensure fair competition.[126] Indeed, OPs have gained an unprecedented economic and *de facto* regulatory power, and commentators stress that, considering their role in the digital economy, and in particular the huge financial and technological resources they can benefit from, the Safe Harbour regime itself should be questioned, as to make OPs accountable for identifying and filtering out illegal content.[127] In this line, it has been noted how intermediaries take an increasingly active role, contributing to frame how third party content is created, accessed, and organised, beyond the purpose of mere intermediation,[128] while judicial and administrative authorities tend to respond to the aforementioned 'liability gap' precisely by adopting a strict interpretation of the 'passive' requirement, as to exclude, in certain circumstances, search engines, social networks and sharing platforms from the safe harbour regime.[129] These tendencies, together with the legal fragmentation in the different implementation and interpretation of the safe harbours described above, as well as the proliferation of new forms of sectoral liability at both national and European level (see §section 6.2-6.10 below) have seriously undermined the capacity of the ECD to ensure legal certainty. Last, but not least, the lack of a Good Samaritan clause is seen as incentivising intermediaries to remain passive in relation to unlawful and/or infringing activities, thus leading to a sub-optimal mediation of online content by the subjects who would be in the best position to fight illegal/harmful activities.[130]

However, despite agreeing that regulatory intervention in the field is needed, some authors believe that the secondary/intermediary liability exception is still justified, because inherently connected to the OPs' function of 'communication enablers' and be merely adjusted to the scenario and challenges. In this sense, Sartor[131] suggests that the new liability exemptions should have a broad personal scope, covering all main intermediaries, including search engines and collaborative platforms, and apply to all intermediation services, both passive and active. In the same line, it is suggested that all kinds of illegal activities that are enabled by the intermediary shall be covered by the safe harbour – including violations of data protection law – as well as good faith removal of inappropriate or irrelevant materials. On the contrary – according to this proposal – the exemption should not cover situations in which the users' illegal behaviour is favoured by the violation of duties resting upon the intermediary – i.e. duties of care, the violation of which may lead to secondary liability –. Also, the exemption should end when the providers know or should have known of the illegitimate activity (presence on the platform plus illegal nature) – thus providing a sort of liability for 'constructive knowledge' – and should not exclude OPs from being subject to orders by competent authorities.

(ii) ELI Model Rules. A possible complement to the 'Safe Harbour' has recently been suggested by the ELI Model Rules on Online Platforms (ELI MRs), developed in 2020 as a 'model for national, European

[125] See Busch, Dannemann, Schulte-Nölke, Wiewiórowska-Domagalska and Zoll (2016). 'Research Group on the Law of Digital Services. Discussion Draft of a Directive on Online Intermediary Platforms.' Journal of European Consumer and Market Law **5**(4): 164-169.; Busch, Schulte-Nölke, Wiewiórowska-Domagalska and Fryderyk (2016). 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law?' Journal of European Consumer and Market Law **5**(1): 3-10; Sartor (2017). Providers Liability.

[126] See Hacker (2018). 'UberPop, UberBlack, and the Regulation of Digital Platforms after the Asociacion Profesional Elite Taxi Judgment of the CJEU.' European Review of Contract Law **14**(1): 80-96, Busch, Schulte-Nölke, Wiewiórowska-Domagalska and Fryderyk (2016). The Rise of the Platform Economy, Research Group on the Law of Digital Services ibid.'Discussion Draft of a Directive on Online Intermediary Platforms.' (4): 164-169. Also see Botta and Wiedemann (2019). 'To discriminate or not to discriminate? Personalised pricing in online markets as exploitative abuse of dominance.' European Journal of Law and Economics: 1-24.

[127] See Sartor (2017). Providers Liability., p. 5

[128] Ibid., p. 5. Gillespie (2018). 'Platforms Are Not Intermediaries.' Georgetown Law Teechnology Review **2**: 198.

[129] Sartor (2017). Providers Liability.

[130] See Lomba and Evas (2020). Digital Services Act. European added value assessment, p. 289.

[131] See Sartor (2017). Providers Liability.

and international legislators as well as a source of inspiration for self-regulation and standardisation' (Article 1.1)[132] of the relationships entertained by information society services[133] with their users, and that will be further analysed in section 6.9.3. Indeed, Article 10 of the ELI MRs suggest that ('PO') shall not have a general obligation to monitor or actively seek facts or circumstances indicating illegal activity. Yet, if they 'obtain credible evidence of (a) criminal conduct of a supplier or customer to the detriment of other users; or (b) conduct of a supplier which is likely to cause physical injury, a violation of privacy, infringement of corporeal property, deprivation of liberty or violation of another similar right to the detriment of another platform users' and yet 'fails to take adequate measures for [their] the protection of the platform user', then the PO 'is liable for damages caused to the platform users [or other persons] as a result of this failure'. Likewise, if a platform operator receives a notification of misleading information presented by suppliers on the platform, it must, in cooperation with the supplier, take reasonable steps to have it rectified, removed or made inaccessible, providing openly accessible means of communication for making the notification, also in an anonymous form.

As the ELI MRs explain, while the first provision Paragraph (1) corresponds and is compatible with Article 15 ECD, the second provision correspond only partially to the one set in Article 14 ECD. In fact, Article 10 imposes a duty to act in the event that the PO obtains credible evidence of illegal conduct that is to the detriment of other users, obliging it to take adequate measures to prevent harm to other users, and holding it liable for the damage caused by its failure to do so. Whereas the ECD sets negative conditions for a harmonised liability exemption, Article 10 sets out some basic obligations for PO, as well as possible sanctions for non-compliance; moreover, it clarifies that such obligations should cover the harm suffered not only by the users of the platform, but also by other persons who come into contact with the platform as well as the goods, services or digital content distributed with its help, whenever they fall under the scope of protection of a platform-user-contract.

6.2 Media Law

Legislative framework. The Audiovisual Media Services Directive and its revision. The AVMSD was originally adopted in 2010[134] to ensure the proper functioning of a single EU market for audiovisual media services. It was aimed at shaping technological developments, create a level playing field for emerging audiovisual media, promote cultural diversity, protect children and consumers, safeguard media pluralism, combat racial and religious hatred, and guarantee the independence of national media regulators.

As part of the Digital Single Market Strategy, the original directive was amended and updated by Directive (EU) 2018/1808,[135] which modifies the regulatory framework as to make restriction directed

[132] See European Law Institute (2019). Report of the European Law Institute. Model Rules on Online Platforms Vienna.

[133] The ELI Model Rules on Online Platforms 'are intended to be used in relation to platforms which: (a) enable customers to conclude contracts for the supply of goods, services or digital content which suppliers within a digital environment controlled by the platform operator; (b) enable suppliers to place advertisements within said digital environment which can be browsed there to contact suppliers and to conclude a contract outside the platform; (c) offer comparison or other advisory services to customers which identify relevant suppliers of goods, services or digital content and which direct customers to those suppliers' websites or provide contact details; (d) enable users to provider reviews regarding suppliers, customers, goods, services or digital content offered by suppliers, through a reputation system'. See ibid., Art. 1(2).

[134] See Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), *OJ L 95, 15.4.2010, p. 1–24.*

[135] See Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, *OJ L 303, 28.11.2018, p. 69–92.*

to TV more flexible, strengthen the protection of European content, increase the effectiveness of measures for children protection and against hate speech, reinforce interdependence of national regulatory authorities, and –– extend certain audiovisual rules to video-sharing platforms as well as audiovisual content shared on certain social media services.

AVMSD aims and two-tiered structure. The directive sets some fundamental principles for regulating audiovisual media services at European level and covers all services with audiovisual content irrespective of the technology used to deliver the content (principle of technological neutrality). It therefore addresses both traditional TV broadcasts, and on-demand audiovisual media services (AVMS).[136] Furthermore, the directive also sets specific rules for video-sharing platform services (VSPS), which are defined as services offering 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, using electronic communication networks, and the organisation of which is determined by the video-sharing platform provider, including by use of automatic means or algorithms, in particular by displaying, tagging and sequencing.

The directive is based on a gradual regulation, as it provides a two-tier system, distinguishing between linear (television broadcasts) and non-linear (on-demand) services. It acknowledges a set of core societal values applicable to all AVMS, provides rules applying online on television broadcasters, and lighter rules for on-demand services where users have an active role, deciding both the content and the time of viewing. As for the general requirements, the directive sets up rules on the 'country of origin principle' – but allows Member States to restrict the reception of certain content that may not be banned in its country of origin but which violates local laws, under the Commission's approval and in exceptional circumstances –, commercial communication, audiovisual advertising, sponsorship and product placement, protection of children, prohibition of incitement to violence or hatred towards discriminated groups, prohibition of public provocation to commit a terrorist offence, improved access for persons with disabilities, designation of EU contact points.

Rules applicable to VSPS. In reference to VSPS, Article 28b of the revised directive requires Member States put in place appropriate measures to:

- protect minors from programmes, user-generated videos and audiovisual commercial communications which could affect their physical, mental or moral development;
- protect the general public from programmes, user-generated videos and audiovisual commercial communications containing:
- provocation to commit a terrorist offence, offences concerning child pornography and offences concerning racism and xenophobia;
- incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter of Fundamental Rights of the European Union;

[136] In this respect, the AVMSD defines audiovisual media service as 'a service providing programmes, under the editorial responsibility of a media service provider, to the general public, to inform, entertain or educate, using electronic communications networks, either broadcast or on-demand, whereas on-demand audiovisual media service are defined as audiovisual media service provided by a media service provider for the viewing of programmes at the moment chosen by the user and at his individual request on the basis of a catalogue of programmes selected by the media service provider' (emphasis added). Thus, the AMSD covers both television broadcasts, and content selected by viewers ('on-demand') over an electronic communications network (typically Connected TV sets, mobile devices or the internet) for watching at a time of their choice, as well as audiovisual advertising, when said contents are provided commercially (i.e. not on private individuals' websites), for the general public (i.e. not including any form of private correspondence), as a programme (i.e. not including websites containing ancillary audiovisual elements such as graphical elements or short adverts), and under the editorial responsibility of a media service provider, who control the selection and organisation of the programmes.

Such measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the VSPS providers, and of the users having created or uploaded the content, as well as the general public interest. Indeed, those measures shall be practicable and proportionate, taking into account the size of the video-sharing platform, and the nature of the service provided, and should not lead to ex-ante control measures or upload-filtering of content, which do not comply with Article 15 ECD.

In particular, such measures shall include, among others, mechanisms and tools for: '(e) establishing and operating systems through which video-sharing platform providers explain to users of video-sharing platforms what effect has been given to the reporting and flagging referred to in point (d); (f) establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors; (g) establishing and operating easy-to-use systems allowing users of video-sharing platforms to rate the content referred to in paragraph 1; (h) providing for parental control systems that are under the control of the end-user with respect to content which may impair the physical, mental or moral development of minors; (i) establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints to the video-sharing platform provider in relation to the implementation of the measures referred to in points (d) to (h); (j) providing for effective media literacy measures and tools and raising users' awareness of those measures and tools'.[137]

Furthermore, the directive requires Member States to extent to VSPS providers the same obligations as audiovisual service providers in respect of advertising and other content restrictions, taking into account the limited control they exercise over advertising on their platforms that is not marketed, sold or arranged by them.

Moreover, the directive requires Member States to ensure that VSPS apply those measures within their jurisdiction, and strongly encourages the adoption of co-regulatory instruments and exchange practices for fighting online illegal content.

6.2.1 Discussion

The inclusion of specific obligations for VSPS constitutes one of the major steps in the current initiatives on increasing the responsibility of OPs for managing and moderating online illegal/harmful content, and, as such, it is widely welcomed.

However, some problematic issues have been highlighted by both academic responses, assessment studies and public consultations.

Critical Issues. (i) Definition of VSPS. Firstly, it is unclear what type of OPs fall within the notion of VSPS adopted by the AVMSD. Indeed, according to Article 1(1)(aa) a VSPS is 'a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, 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 within the meaning of point (a) of Artide 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing'.[138] Against this vague definition, the major difficulty lays in understanding when one

[137] See Art. 28b (3) AVMSD.

[138] See Gawer (2016). Online Platforms: Contrasting perceptions.

service's 'essential functionality' is devoted to the provision of programmes, users generated videos, or both, to the general public.

Under its responsibility set forth by recital 5, the Commission has issued guidelines on the matter,[139] suggesting that Member States should identify the essential functionality of the services – i.e. the fact that the audiovisual content is not 'merely ancillary to, or a minor part of' the activities of the service concerned' – on the basis of four indications:

- *The relevance of the audiovisual content for the main economic activity or activities of the service*, which can be established with reference to: the overall architecture and external layout of the platforms; the stand-alone nature of the audiovisual content; the specific functionalities of the services tailored for, or specific to, audiovisual content; the way the service positions itself on the market and the market segment it addresses;
- *The quantitative and qualitative relevance of the audiovisual content available on the service*, which is demonstrated by the amount of audiovisual content available on the platform, the measure of its use and as well as of its public reach;
- *The revenue generated from the audiovisual content*, which can be inferred from: the inclusion of commercial communications in or around audiovisual content; the fact that access to audiovisual content is subject to payment; the presence of sponsorship agreements between brands and uploaders, the tracking of users' platforms activities for commercial purposes;
- *The availability of tools aimed at enhancing the visibility or attractiveness of the audiovisual content*, such as actions and features promoting the consumption of audiovisual material, the presence of tools available within or around the videos that are designed to attract users and encourage their interaction, or tools/systems allowing users to select the audiovisual content they wish to be offered, or tools/systems that track the performance and manage content uploaded on the platforms.

Despite their relevance, these guidelines are not legally binding, and – despite also encouraging forms of exchange and coordination among Member States, as well as between national authorities and OPs – do not ensure the uniformity of interpretation and implementation among Member States. This, together with the case-by-case nature of assessment on the applicability of the AVMSD to each VSPS, substantially limits the certainty of the legal regime, thus affecting the directive's capacity to shape OPs' responsibility to ensure a safe digital environment.

(ii) Limited scope. Likewise, the Directive has a limited objective scope, as it addresses only specific types of illegal and harmful content (protection of children, prohibition of incitement to violence or hatred, or public provocation to commit a terrorist offence), and in this sense it can be seen as complementary to the vertical regulations extant in these fields.

6.3 Online piracy, IP and copyright infringements

IP Law: sectors and functions. Intellectual property (IP) law covers intangible creations of the human intellect and comprises rules on copyrights, trademarks, patents, and trade secrets. It contrasts illegal and harmful phenomena such as online piracy – unauthorised distribution of copyright-protected content over the internet – by granting copyright holders a temporary monopoly in the distribution

[139] See Communication from the Commission Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service' under the Audiovisual Media Services Directive 2020/C 223/02, C/2020/4322, OJ C 223, 7.7.2020, p. 3–9.

and exploitation of their protected work, with limited exemptions on temporary use in case of legitimate interests.

Online infringements of IP law. OPs represent a prolific environment for the diffusion of material infringing IP law, posing significant threats to businesses, IP rights holders, consumers and society in general. The sale of counterfeited products on online marketplaces or the promotion of websites selling such goods through browsers' advertisement services, for example, is a complex phenomenon that involves the production, distribution and sale of fake products, amounting to several IP infringements – e.g. trademark, patent and copyright – in addition to potential non-observance of other applicable regulation (e.g. in the sale of counterfeited medicines). Because of the significance of such a threat, the EU has stepped up to address the matter, increasing OPs overall responsibility to fight online-distribution of copyrighted content online.

Legislative framework: (i) Directive 2019/790 on Copyright and related rights in the Digital Single Market. Directive 2019/790[140] (CDSM) sets important updates to the directives constituting the IP law framework.[141] *Inter alia*, it introduces new mandatory exceptions allowing the use of copyright-protected material; establishes extended collective licensing and negotiation mechanisms for making audio-visual works available on video-on-demand platforms; grants new rights to EU-based press publishers working through online service providers for the digital use of their press publications; and entitles authors and performers to receive regularly up-to-date, relevant and comprehensive information on the exploitation of their works and performances.

Most importantly, Article 17 of the directive prescribes that online content-sharing service providers (OCSSP) must obtain permission from rightsholders to make works uploaded by their users available to the public, for example through a licensing agreement. If a licence agreement is not concluded, the platforms may benefit from a liability-mitigation mechanism only if they make 'best efforts' to ensure that unauthorised content is not available on their websites, based on the information provided by the rightsholders.

Moreover, the directive also requires OCSSP to adopt procedural safeguards to minimise the risks of broad filtering and over-blocking. Indeed, they are under an obligation to put in place rapid and effective measures that can enable users to lodge a complaint against the blocking or removal of content. Complaints shall be processed without undue delay, and decisions to disable access to or remove uploaded content shall be subject to human review.

(i) Injunctions. The Directive 2004/48/EC on the enforcement of intellectual property rights (IPRED)[142] aims at providing a level playing field on the enforcement of IP rights, while the Directive 2001/29/EC aims to adapt legislation on copyright and related rights to technological developments, and particularly to the information society (Infosoc),[143] and both enact important mechanisms for the

[140] See Directive (EU)2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, pp. 92-125).

[141] Namely: 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 OJ L 167, 22.6.2001, p. 10–19; and the directives on: the enforcement of intellectual property rights (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157, 30.4.2004, p. 45–86); orphan works (Directive 2012/28/EU of the European Parliament and of the Council of 25 October 2012 on certain permitted uses of orphan works, OJ L 299, 27.10.2012, p. 5–12); and the collective management of copyright and related rights (Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market, OJ L 84, 20.3.2014, p. 72–98).

[142] See Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157, 30.4.2004, p. 45–86.

[143] See 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, *OJ L 167 22.6.2001, p. 10–19.*

protection of IP rights against infringements online. Article 9 (1) a) of the IPRED provides that judicial authorities may issue interlocutory injunctions against an intermediary whose services are used by a third-party to infringe such rights. Article 8 (3) of the Insofoc, instead, provides that injunctions may be issued against an intermediary whose services are being used by a third party to infringe IP rights aimed at prohibiting the continuation of the infringement. The CJEU has further clarified that such an injunction can be aimed not only at stopping the infringement but also at preventing such infringement, without the latter resulting in a general monitoring obligation that would, instead, violate Article 15 ECD.[144]

The IPRED evaluation carried out by the EC showed that 'different notions of 'intermediary' are used at national level'.[145] In response to that, the EC issued specific Guidelines on the interpretation of the IPRED, and it clarified that any economic operator which provides services capable of being used by other persons to infringe IP rights can fall within the scope of the IPRED's notion of intermediary.[146] Thus, OPs such as online marketplaces and social networking platforms fall within the notion of intermediaries and may be potentially subject to injunctions.[147]

Injunctions against online platforms/intermediaries are not liability-dependent and thus may be issued against an innocent intermediary.[148] In this sense, they mirror the provision set in Article 14 (3) of the ECD, according to which the exemption of liability applicable to hosting providers does not limit the authorities' possibility of requesting termination or prevention of the infringement to the hosting provider. However, said injunctions cannot amount to a general monitoring obligation, contrary to Article 15 of the ECD, as decided by the CJEU in the *Sabam* case.[149]

Voluntary initiatives and codes of conduct. (i) Ad-funded IP infringement. One of the major problems of tackling online copyright infringements is raised by websites that offer consumers infringing content online (i.e. books, films, music, etc.) for free. These websites generate a high web user traffic that is afterwards capitalised by selling the advertising space of their webpages to advertisers in general, and

[144] See C-324/09 L'Oréal SA and Others v eBay International AG and Others, EU:C:2011:474, para. 131.

[145] See Public consultation on the evaluation and modernisation of the legal framework for the enforcement of intellectual property rights launched on 9 December 2015, results available at http://ec.europa.eu/DocsRoom/documents/18661. European Commission (2017). Commission staff Working Document. Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights. SWD(2017) 431 final Brussels, European Commission. , pp. 12 and 21.

[146] Ibid., p. 13.

[147] See C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, EU:C:2012:85, para. 28; C-324/09 L'Oréal SA and Others v eBay International AG and Others, EU:C:2011:474, para. 131.

[148] C-324/09 L'Oréal SA and Others v eBay International AG and Others, EU:C:2011:474, para. 127. Also see Nordemann (2020). The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services Luxembourg, Policy Department for Economic.

[149] See Case See C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, EU:C:2012:85, where the CJEU stated that a national court cannot issue an 'injunction against a hosting service provider which requires it to install a system for filtering:– information which is stored on its servers by its service users; – which applies indiscriminately to all of those users; –as a preventative measure; – exclusively at its expense; and – for an unlimited period, and which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright'. On this type of liability, also see Husovec (2017). 'Injunctions against Intermediaries in the European Union: Accountable but Not Liable? of Entry.' Injunctions against Intermediaries in the European Union: Accountable but Not Liable? of WebLog 2017.

advertising intermediaries in particular,[150] earning as much as EUR 5.5 million each annually.[151] To tackle this issue, the most recent initiatives aim precisely at drying up the digital advertising revenue streams of these websites, according to the so-called 'Follow the Money' approach. Indeed, on June 2016, under the EC's aegis, a group of advertisers, advertising agencies, trading desks, advertising platforms, advertising networks, advertising exchanges, publishers and IP rights owners signed the Memorandum of Understanding on online advertising and intellectual property rights[152] (MoU) to minimise the placement of advertising on websites and mobiles apps that infringe copyright or disseminate counterfeit goods.[153] On the basis of their individual policies and assessment criteria, signatories should 'limit the placement of advertising on other websites and/or mobile applications, which have no substantial legitimate uses and for which advertisers have reasonably available evidence that these websites and applications are infringing copy-right or disseminating counterfeit goods on a commercial scale[154]. Moreover, the MoU sets forth particular obligations for advertising Intermediaries,[155] requiring them to (i) make sure that their contractual terms allow for the use of tools for content verification, advertising delivery and reporting so that advertising is not placed on IP rights infringing websites; (ii) take reasonable steps for the removal of such ads once identified; (iii) adopt IP rights policies describing the tool and measures adopted for complying with the MoU; (iv) report annually to the Commission and other signatories on the steps undertaken to comply with the MoU and their effectiveness. Indeed, all signatories are obliged to cooperate with the EC in assessing and reporting on the MoU. On August 2020 the Commission published the first report on the implementation of the MoU which shows, among others, that: (i) the signatories have agreed that the MoU promotes good practice and is operating satisfactorily due to the commitment of the participants to make it work; (ii) the share of advertisements of European business on IP rights-infringing websites has dropped by 12%, and advertising by major brands has decreased from 62% to 50% in the gambling sector and downward trends related to EU major brands and EU ad intermediaries have also been identified; (iii) signatories consider that there is no apparent need to amend the text of the MoU as its provisions have been drafted in such a way as to incorporate new initiatives and take into account new trends within the framework of the MoU; and (iv) sharing expertise, strengthening cooperation with public authorities, and raising awareness, at national, EU and international level would be crucial to spread good practice and facilitate adherence to the MoU.[156]

---

[150] See Office for Harmonization in the Internal Market (2016). Digital Advertising on Suspected Infringing Websites. p.15. The advertising industry has changed substantially with the increasing levels of automation and new intermediary players have emerged which now control how and when adds are being placed. Initially, brands purchased the advertising space (multiples ad spaces are called Inventories) from the websites/publishers directly. Each time and ad is viewed in an advertising space on a website is called an 'Impression'. Websites sell millions of such Impressions which led to the creation of Ad Networks which buy unsold Impressions, aggregate such Impressions in Inventories which are then sold to the brands or their agencies. This carries on to what is called an Ad Exchange which is an online marketplace where inventories are published for sale and then bought by ad networks, brands and agencies. These transactions are carried out by algorithms which match the advertisers with the websites in milliseconds. This in turn, increases the risks of ads being placed on infringing websites and brands losing control over their advertising space.

[151] ibid., p. 5.

[152] See (2018). 'Memorandum of Understanding on online advertising and intellectual property rights.'. The MoU is not legally binding and it does not create any contractual or pre-contractual liability or any rights or obligations, although the signatories commit to undertake the actions provided for by the MoU. The 'sanction' for non-compliance is expulsion or as the MoU states 'an invitation to withdraw' from the MoU. See ibid., pp. 2 and 5.

[153] See ibid., p. 1.

[154] See ibid., p. 2.

[155] Advertising intermediaries are defined as 'signatories directly involved in buying, selling or brokering the sale or purchase of advertising space'. See ibid., p. 3.

[156] See European Commission (2020). Commission Staff Working Document. Report on the functioning of the Memorandum of Understanding on online advertising and intellectual property rights. SWD(2020) 167 final/2 Brussels, European Commission. , p. 14. Also see White Bullet Solutions Limited (2020). Study on the impact of the Memorandum of

(ii) Sale of counterfeit goods in online marketplaces. In 2011 major online platforms, associations and rights holders, with the facilitation of the European Commission, signed the Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet[157] as a voluntary tool meant to prevent offers of counterfeit goods from appearing in online marketplaces by improving NTD measures and proactive measures. The MoU was revised and signed again in 2016 to include key performance indicators for tracking and measuring the MoU's success.

The European Commission published so far three reports on the implementation of the MoU.[158] The latest report shows that the MoU is a useful and efficient tool in counteracting the sale of counterfeit goods on the internet and that 'voluntary cooperation can provide the flexibility to discuss and deliver efficient solutions'.[159] The MoU's greatest perceived benefit is that of its functioning as a 'laboratory' where the signatories can 'exchange practical examples of practices on proactive and preventive measures, NTD procedures and ways to share information e.g. on repeat infringers'. However, certain drawbacks have been reported by the signatories, other than online platforms such as:[160] (i) 'signatories consider the cooperation and information exchange with online platforms to fall short of the commitments made under the MoU', and (ii) 'signatories questioned the usefulness of directly comparing quantitative data provided through the KPI windows seeing the dynamics of the collection exercise, differences in methodology and the lack of reliable auditing'. Moreover, in June 2020 three rights owners in the fashion and luxury goods sectors decided to withdraw from the MoU, as they believe that progress is not sufficient, and the level of counterfeit offers is still too high. Overall, the conclusion is that although the MoU has provided certain benefits, its effectiveness is impacted by the low number of OPs signatories and sometimes their lack of involvement, and that future actions should not focus on the text of MoU but on how attract a higher degree of involvement and action.

6.3.1 Discussion

Shift from secondary to primary liability. Historically, the liability of information society services providers was regulated as secondary or intermediary liability. Nevertheless, given the increasing role of OPs in providing access to content online, the EU legal framework is heading towards a primary liability regime, as the regime set out in Article 17 CDSM clearly demonstrates.

The article states that when online content services providers (OCSP) – 'provider[s] 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'[161] – diffuse the copyright-protected works uploaded by their users, they 'communicate or make available to the public' such materials, and thus

Understanding on online advertising and intellectual property rights on the online advertising market Brussels, Directorate-General for Internal Market.

[157] See (2011). The Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet.

[158] See European Commission (2013). Report from the Commission on the functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet. COM(2013) 209 final Brussels, European Commission. ; European Commission (2017). Overview of the functioning of the Memorandum of Understanding on the sale of counterfeit goods via the internet. SWD(2017) 430 final Brussels, European Commission. ; European Commission (2020). Commission Staff Working Document. Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet. SWD(2020) 166 final/2 Brussels, European Commission.

[159] See COM SWD(2020) 167 final/2, p. 37.

[160] See ibid., pp. 37-38.

[161] See Art. 2 (6) CDSM. This definition is mirrored by recital 62 CDSM, stating that 'the services covered by this Directive are services, the main or one of the main purposes of which is to store and enable users to upload and share a large amount of copyright- protected content with the purpose of obtaining profit therefrom, either directly or indirectly, by organising it and promoting it in order to attract a larger audience, including by categorising it and using targeted promotion within it'.

need specific authorisation to do so.[162] Otherwise, they would be in breach of IP law, and will not benefit from the exemption under Article 14 (1) ECD. However, the providers will be able to escape liability if they demonstrate that they: (a) made best efforts to obtain an authorisation, and (b) in accordance with high industry standards of professional diligence, made best efforts to ensure the unavailability of specific works and other subject matter for which the rights holders have provided the OCSP with the relevant and necessary information; and in any event (c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b). If, despite such efforts are employed, unauthorised works still become available and OCSP were provided with the relevant and necessary information from rightsholders to remove such works, then they will be able to escape liability if and when they proved that they have made the required best efforts to ensure the unavailability of specific works.

Article 17 puts forth a fault-based liability where the fault is that of a highly diligent provider. That entails considering all the steps a diligent operator would have taken to prevent the availability of unauthorised works or other subject-matters on its website, taking into account best industry practices and all relevant factors and developments, such as the size of the service, the evolving state of the art, and potential future developments.[163] Moreover, providers could still be liable when failing to act expeditiously in removing infringing content after being provided with a substantiated notice in this respect and failed to prevent the reappearance of such unauthorised content.

However, providers will not be considered at fault if rightholders had not provided them with the relevant and necessary information on their specific works or other subject matter, or failed to notify the disabling of access to, or the removal of, specific unauthorised works, as this prevents service providers from complying with their duties.[164] Although the CDSM provides for a total exclusion of liability, in practice the liability will be apportioned taking into account rightholders' contribution and failure to promptly act to mitigate damages. In any case, the measures to be demanded of OPs, be it preventive or dissuasive in nature, may not amount to a general monitoring obligation.

Interpretative problems related to Article 14 and 15 ECD. If art 17 CSMD certainly constitutes the major development in the field, it is important to stress that it only applies for specific types of OPs – those qualifying as OCSSP –, whereas the others still fall within the application of the harmonised conditions for liability exemptions under Article 14-15 ECD. Yet, the same tendency to shift from a conditional secondary liability to a regime of primary liability based on fault can still be found even within this broader and general field of regulation. Indeed, some scholars claim that, over the years, the CJEU has developed a rather extensive reading of the conditions limiting OPs' liability exemptions under Article 14 ECD. Indeed: (i) the fact that the OPs' overall economic operation is profit-based is considered as sufficient for meeting the 'profit-making' requirements qualifying the distribution of copyright-protected material as a breach of IP law (instead of focussing on financial interests of the specific act of communication to the public); (i) the OPs were considered precluded from the liability exemption, when the operator 'could not be unaware' about the fact that users published copyrighted materials without the consent of the rightholders, thus including in the concept of knowledge on the illicit nature of the activity carried out over the platform as a form of 'constructive knowledge'.[165] In this sense, it has been claimed that 'operators of platforms with a profit-making intention would have an *ex ante* reasonable duty of care and be subject to an *ex post* notice-and-takedown system, which would

[162] See Case C-610/15 Stichting Brein, EU:C:2017:456.

[163] See Recital 66 CDSM.

[164] Ibid.

[165] Rosati (2020). The Direct Liability of Intermediaries. Oxford Handbook of Online Intermediary Liability. Frosio. USA, Oxford University Press.

also include an obligation to prevent infringements of the same kind, for example by means of re-uploads of the same content'.[166] However, this interpretation is not univocal, and rather describes the extent of uncertainties over OPs' specific obligations and liability for illegal/harmful content, possibly incentivising OPs to voluntarily engage in comprehensive-monitoring and over-removal strategies, in violation of users' fundamental rights and freedoms.[167]

6.4 Child Protection

Children's vulnerability online. Minors of ever younger age make massive use of OPs and specific attention shall be devoted to the protection of their safety and wellbeing online. Indeed, over the Internet children can be exposed to harmful material (e.g. pornographic and violent content, or content promoting different types of self-harm), harmful behaviour (e.g. cyberbullying) and harmful contact (e.g. sexual harassment, grooming), and measures are required to prevent negative consequences for their cognitive, social and emotional development. Use of personal data and advertisement practices may also be dangerous since children often lack the knowledge, awareness and overall capacity to engage critically with it.[168] Moreover, the Internet constitutes a prolific and often anonymous environment for the production and consumption of child-abuse-related and pedo-pornographic content, as it offers broad distribution channels, facilitates anonymity and feeds vicious circles on the victimisation of children, leading to vast and long-lasting harms.[169]

For these reasons, a series of initiatives have been taken at the EU level, comprising:

- soft law instruments and the setting up of bodies deputed to the monitoring, coordination and overall management of soft-law and voluntary initiatives;
- the adoption of legislative instruments designed precisely for protecting children, e.g. to combat crimes perpetrated against them (e.g. child abuse and child pornography);
- the provision of specific rules for minors within the regulation of broader and transversal topics (e.g. in the GDPR and in AVMSD; see section 6.2 and section 6.10).

Soft law and voluntary initiatives: (i) The European Strategy for a Better Internet for Children. Within the policy initiatives, particularly important is the European Strategy for a Better Internet for Children,[170] which connects EU Institutions, Member States, and representatives of the industry – including providers of social networking services – to ensure high quality of online content for children and young people, foster their awareness and empowerment (e.g. promoting data literacy and simple yet robust reporting tools), and create a safe environment (e.g. through age-appropriate privacy settings, wider use of parental control and age rating and content classification). In particular, the strategy steps up to combat child sexual abuse material online and child sexual exploitation, through faster and systematic identification and take-down of the material disseminated through various channels, and instruments for cooperation with international partners.

[166] See ibid.; Leistner (2017). 'Closing the book on the hyperlinks: brief outline of the CJEU's case law and proposal for European legislative reform.' European Intellectual Property Review 39(6): 327-333.

[167] See Senftleben (2020). Oxford Handbook of Online Intermediary Liability. Intermediary Liability and Trade Mark Infringement: Proliferation of Filter Obligations in Civil Law Jurisdictions? Frosio. Oxford, Oxford University Press**:** 382-402.

[168] See European Data Protection Board (2020). Guidelines 8/2020 on the targeting of social media users., p. 7.

[169] See OECD (2019). An Introduction to Online Platforms., p. 118; Secretary of State for Digital Culture Media & Sport and Secretary of State for the Home Department (2019). Online Harms White Paper UK. , p. 5.

[170] See European Commission (2012). Communication from the Commission. European Strategy for a Better Internet for Children. COM(2012) 196 final Brussels, European Commission.

(ii) Safer Internet Centres and Alliance to better protect minors online. An important instrument in the fight against child-related harmful/illegal material online is represented by the Safer Internet Centres, constituted in each Member States and coordinated by the Commission through a single entry point (the Better Internet for Kids portal), which aims to raise awareness and foster digital literacy among minors, parents and teachers, and fight child-related crimes through a network of hotlines (INHOPE).[171]

(iii) Self-regulatory bodies and instruments. As for self-regulatory initiatives, the Alliance to better protect minors online is a self-regulatory tool supported by the Commission and featuring leading ICT and media companies, civil society and industry associations tackling harmful online content and behaviour,[172] including harmful content, conduct and contact which children may experience online. The Alliance's members signed a common Statement of Purpose, committing to three main goals: user-empowerment (e.g. through appropriate feedback and notification systems and content classification tools), awareness-raising (e.g. media literacy); and promotion of children's access to diversified online content, opinions, information and knowledge. [173]

Similarly, the joined EU and US initiative Global Alliance against Child Sexual Abuse Online and WeProtect Global Alliance[174] commit to ensuring a larger number of rescued victims, more effective prosecution, and an overall reduction in the number of child sexual abuse images available online. Due to the broadness of the Alliance's member base and the relative abstract-nature of its goals, members are supposed to focus on those commitments that are directly relevant to the risks and concerns that are more relevant for their activity. Following an agreement with the Commission, the work of the Alliance has been subject to evaluation through independent reports.[175]

Regulatory framework. (i) Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography. As for the legislative layer, Directive 2011/93[176] obliges Member States to adopt preventive measures against sexual abuse and sexual exploitation of children and child pornography, to protect child victims, as well as to investigate and prosecute offenders.[177] Most importantly, the directive requires Member States to ensure the prompt removal of web pages containing or disseminating child pornography in their territory, and to work to obtain removal if

[171] See https://ec.europa.eu/digital-single-market/en/content/creating-better-internet-kids-0.

[172] See (2017). A Safer Internet for Minors. Statement of Purpose Alliance to Better Protect Minors Online. Company signatories are : ASKfm, BT Group, Deutsche Telekom, Disney, Facebook, Google, KPN, The LEGO Group, Liberty Global, Microsoft, Orange, Rovio, Samsung Electronics, Sky, Snap, Spotify, Sulake, Super RTL/Mediengruppe RTL Deutschland, TIM (Telecom Italia), Telefónica, Telenor, Telia Company, Twitter, Vivendi, Vodafone. Associated members: BBFC, Child Helpline International, COFACE, eNACSO, EUN Partnership, FFTelecoms, FOSI, Foundation T.I.M. (Against Internet Misconduct), FSM, GSMA, ICT Coalition, NICAM, Toy Industries of Europe, UNICEF. See https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online#:~:text=%20Alliance%20to%20better%20protect%20minors%20online%20,on%20the%20way%20forward%20for%20the...%20More%20.

[173] See ibid., p. 4.

[174] See https://www.weprotect.org/our-mission-and-strategy.

[175] See https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/child-sexual-abuse/global-alliance-against-child-abuse_en.

[176] See Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, p. 1–14

[177] Indeed, Directive 2011/93/EU sets a number of significant criminal rules to criminalise and punish sexual abuse and exploitation, prevent crimes, investigate and prosecute offenders, and to ensure the highest protection to child victims. To protect child victims, it introduces rules on extensive assistance and support measures for child victims; access to assistance and support as soon as there are reasonable grounds to suspect offence; special protection for children reporting abuse within the family; making assistance and support not conditional on cooperation with criminal proceedings; protection of a victim's privacy, identity and image.

hosted outside their jurisdiction, also allowing blocking measure to prevent abuse. According to Article 25, these measures may be of legislative or non-legislative nature, as long as they are adequate for the attainment of the goals set therein. They must be set by transparent procedures and provide adequate safeguards, ensuring that restrictions are necessary and proportionate, that users are informed of the reason for the restriction, and that the possibility of judicial redress is granted.

(ii) Audiovisual Media Services Directive. Moreover, specific provisions for the protection of children online were set in the revised AMSD (discussed in section 6.2 above) whose Article 28(b) obliges Member States, *inter alia,* to ensure that video-sharing platforms adopt and implement appropriate measures to 'protect minors from programmes, user-generated videos and audiovisual commercial communications which could affect their physical, mental or moral development'. As already explained, such measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected, as well as the rights and legitimate interests at stake, including those of the VSPS providers and the users having created or uploaded the content as well as the general public interest. They must be practicable and proportionate, considering the size of the platform and the nature of the service provided, and shall not lead to any ex-ante control measures or upload-filtering of content. They may include, among others, mechanisms and tools for: explaining the effect of the reporting and flagging systems; establishing and operating age verification systems, and systems allowing users of video-sharing platforms to rate content and to set parental controls; providing procedures for the handling and resolution of users' complaints and for promoting media literacy and raising users' awareness of those measures and tools.[178]

Furthermore, the directive requires Member States to extend to VSPS providers the same obligations as audiovisual service providers in respect of advertising and other content restrictions, some of which deal specifically with advertisement targeted to children.

6.4.1 Discussion

Critical issues. Preference over self-regulatory and user-empowerment solutions, legal fragmentation and lack of clear obligations for OPs. Indeed, an overall assessment of the instruments adopted to fight child-related harmful/illegal content shows two main tendencies. Firstly, there is a general preference for self-regulation, public awareness-raising, technological tools/solutions and financial support over legislation, while the latter is primarily directed to the fight against child sexual abuse online. Secondly, hard law regulation tackling child sexual exploitation only sets minimum harmonisation of the tools and techniques to be adopted by Member States for fighting child-abuse related content, leaving a substantially fragmented scenario.

Moreover, when OPs are called to act against illegal/harmful material, no clear guidance is given on how they should meet their responsibilities, especially considering that these measures shall remain compatible with digital intermediaries' liability exemptions under the ECD. [179]

Commission assessments on the implementation of Article 25 Directive 2011/93. In 2016, the European Commission assessed the measures introduced concerning websites containing or disseminating child pornography under article 25(1) of the directive.[180] The report found that Member

[178] See Art. 28b (3) AVMSD.

[179] See C(2018) 1177 final.

[180] See European Commission (2016). Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. COM(2016) 872 final Brussels, European Commission.

States have adopted two types of measure for removing pedo-pornographic material hosted within the territory:

- Measures based on the ECD, setting NTD procedures to remove illegal content, relying on the national hotlines network under the INHOPE system. Depending on the law and procedures applicable within each Member States, enforcement authorities may determine the hosting location, analyse the content and inform the hosting provider, who may be held liable if it fails to remove the content. In Italy, for example, hotlines cannot analyse the content, and merely forward the report of the notice to OPs, which assess it and act accordingly.
- Measures based on criminal law for the seizure of the material relevant to criminal proceedings and the removal of child pornography, possibly in coordination with the NTD measure described above.

As for the provision under Article 25(2), it found that half of the Member States chose to apply optional blocking measures, following – depending on the cases – a mandatory court order, a mandatory request from authorities, or voluntary compliance with the latter, while the use of blacklists is also common. Similarly, the procedures and safeguards adopted differ significantly among Member States.

Overall, the report welcomes the steps adopted and the results achieved – '93% of the child sexual abuse material processed by the hotlines in Europe and 91% of the material processed by the hotlines worldwide was removed from Internet public access in less than 72 hours' – but highlights the need for continuous work towards the complete and correct implementation of the Directive. Thus, the Commission commits to 'sustain and develop multi-stakeholder engagement processes aimed at finding common solutions to voluntarily detect and fight illegal material online and […] reviewing the need for formal notice and take down procedures',[181] confirming the preference over the self-regulatory solutions identified above.

Limited effectiveness of soft-law and user-empowerment initiatives. Despite the positive initiatives undertaken by EU Institutions and stakeholders, the soft-law and user-empowerment oriented approach has been subject to substantial critiques, in particular concerning its adequacy and effectiveness. Livingston and Goodman,[182] for example, noted that the tools adopted to contrast harmful material are insufficient, not broadly shared, and rely too much on users' understanding of complex options and tools. Against this analysis, they argue for a comprehensive Code of Conduct for the converged digital environment setting minimum standards for providers of services used by children, to be embedded according to the by-design approach, with strong backstop powers, independent monitoring and evaluation, and a trusted and sufficiently-resourced body to ensure compliance. Likewise, they suggest the adoption of a Recommendation promoting an integrated approach to media literacy, to be constantly updated and applying consistently through all relevant EU policies, and the setting up of tools and bodies for collecting data regularly to ensure robust and up-to-date guidance on the development of EU policy on the protection of minors in the digital age.

Study evaluating the Alliance. Indeed, even a recent evaluation of the Alliance[183] stressed that there is 'unrealised potential to foresee, discuss and forge common solutions across different stakeholder types, including on existing and emerging threats to the safety of minors online'. In particular, the

[181] See ibid., p.12.

[182] See Livingstone, Tambini, Belakova and Goodman (2018). Protection of children online: does current regulation deliver? London. , Goodman and Livingstone (2018). 'Protection of children online: does current regulation deliver?' https://blogs.lse.ac.uk/medialse/2018/11/27/protection-of-children-online-does-current-regulation-deliver/ 2020.

[183] See Ludden, Hahn and Jeyarajah (2018). Evaluation of the implementation of the Alliance to better protect minors online, Directorate-General of Communications Networks. , p. 5.

stakeholders' participation is deficient – having a non-sufficiently diversified member base, and lacking informal and activity-specific occasion for exchange and discussion –, and the commitments taken are not sufficiently specific, measurable, attainable and timely (SMART). Indeed, it is difficult to assess the degree of their implementation, sector-specific features of the stakeholders involved are not accounted for, and the threat for non-compliance or under-performance is minimum. Against this picture, companies' desire to engage in the protection of minor seems primarily influenced by internal and customer interests, and, as a consequence, voluntary commitments merely reaffirm activities already implemented at the company level and focus on objectives –education, empowerment and awareness-raising –, bearing limited disruptive effect. Against this background, the independent study proposes:

- The revision, clarification and update of the initiative and the elaboration of SMART commitments to be constantly updated;
- The re-assessment and broadening of the Alliance's composition and a revision of its membership policy to increase transparency around the governance, also by establishing working groups as a means for allowing greater interaction and tackling of more narrow-tailored and better-targeted issues;
- The elaboration of a more effective communication plan;
- The creation of a repository of good practices including safety policies, partnership and joint initiatives (e.g. on labelling minor-appropriate content), awareness-raising and user empowerment activities.

However, the study questions the overall effectiveness and the appropriateness of self-regulation, and claims that if no positive results emerge in the next evaluation, EU legislation should be considered as a better means to achieve the aim of protecting children online.

6.5 Hate Speech

Hate speech. Definition. Hate speech covers 'all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, antisemitism or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin'.[184] As such, it is intrinsically connected to the fight against discrimination, prohibited by Article 14 of the European Convention on Human Rights, and under Article 21 (1) of the Charter of Fundamental Rights of The European Union.[185]

Regulatory framework. (i) Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law. At the regulatory level, the fight against hate speech is pursued through the Framework Decision 2008/913/JHA,[186] which aims to ensure that in all Member States serious manifestations of racism and xenophobia committed within the territory of the EU, by an EU national, or for the benefit of a legal person established within the EU,

[184] See Rosenfeld (2002). 'Hate speech in constitutional jurisprudence: a comparative analysis.' Cardozo Law Review **24**(4): 1523-1467., p. 10.

[185] See Art. 21 (1) of the Charter of Fundamental Rights of The European Union: 'any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited'. Mapping all international instruments applicable to hate speech exceeds the purpose of this study. However, for a full mapping see Bayer, Bard and Lorand (2020). Hate speech and hate crime in the EU and the evaluation of online content regulation approaches Lexembourg, Affairs. .

[186] See Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, *OJ L 328, 6.12.2008, p. 55–58.*

are punishable through effective, proportionate and dissuasive criminal penalties, and to foster judicial cooperation to this end.[187] The Decision qualifies as punishable criminal offences a series of action related to hate speech, as well as their instigation, aiding or abating (public incitement to violence or hatred directed against a group of persons or a member of such a group defined on the basis of race, colour, descent, religion or belief, or national or ethnic origin).[188] Despite its general importance, the Decision does not deal specifically with hate speech online, leaving a serious regulatory gap. Indeed, the 2014 Implementation report published by the Commission,[189] showed that due to its special character, including the difficulty of identifying the authors of illegal online content and removing such content, hate speech on the internet creates special demands on law enforcement and judicial authorities in terms of expertise, resources and the need for cross-border cooperation.

(ii) Audiovisual Media Services Directive. Against this background, specific provisions for hate speech online were set in the revised AVMSD which obliges Member States to ensure that video-sharing platforms adopt and implement appropriate measures to 'protect the general public from programmes, user-generated videos and audiovisual commercial communications containing incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter',[190] and to 'protect the general public from programmes, user-generated videos and audiovisual commercial communications containing incitement to racism and xenophobia'.[191] A complete analysis of the directive and the measures required under Article 28(b), can be found in section 6.2 above.

National law. At the national level, Germany passed on 1 October 2017 a law against fake news and hate crimes in social networks, i.e. the Network Enforcement Act, also known as NetzDG.[192] The law forces social networks[193] to ensure that 'obviously unlawful content' such as hate speech[194] is deleted within 24 hours as of notice, and requires all platforms that receive more than 100 complaints per calendar year about unlawful content to publish bi-annual reports on their activities. Meanwhile, in June 2020, the French Parliament adopted *Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*,[195] which obliged platform operators and search engines to remove offensive content – incitement to hate or violence and racist or religious bigotry – within 24 hours or

[187] See Recitals 5 and 13 and Art. 3 and Art. 6 under the Framework Decision 2008/913/JHA.

[188] See Art. 1(1) and Art. 2 under Framework Decision 2008/913/JHA. Regarding hate crime, the Decision prescribes that, in all cases, racist or xenophobic motivation shall be considered to be an aggravating circumstance or, alternatively, the courts must be empowered to take such motivation into consideration when determining the penalties to be applied (See Art. 4 Framework Decision 2008/913/JHA).

[189] See European Commission (2014). Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law. COM(2014) 27 final Brussels, European Commission. , p. 9.

[190] Art. 28b (1) b) AVSMD. Reference is expressly made to content to groups identified by the reference to their 'sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation'.

[191] Art. 28b (1) b) AVSMD.

[192] Available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Also see Engels and Fuhrmann (2018). 'Network Enforcement Act in a nutshell.' https://blogs.dlapiper.com/iptgermany/2018/01/31/network-enforcement-act-in-a-nutshell/ 2020.

[193] The law defines social networks as follows: '*telemedia service providers which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public*' (official translation by German Ministry of Justice). See Heldt (2019). 'Reading between the lines and the numbers: an analysis of the first NetzDG reports.' Internet Policy Review **8**(2).

[194] Hate speech as such is not defined by the NetzDG. See ibid., For an analysis on the notion of hate speech and Germany's regulatory constitutional framework see Rosenfeld (2002). Hate speech in constitutional jurisprudence.

[195] See Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet available at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970

risk a fine of up to €1,25 million. However, the *Conseil constitutionnel* has recently stroke down this deadline: according to the French Constitutional court, such provision resulted in an unconstitutional violation of the users' freedom of expression, because it circumvented the court system, turning law enforcement agencies into the judge of what would be legal or illegal content in these matters, and did not provide enough time for online platforms to adequately judge the legality of the content, especially given the risk that they would be flooded by notifications from users.[196]

Self-regulation. Code of Conduct on Countering Illegal Hate Speech Online. In May 2016, the Commission agreed with a group of prominent OPs[197] on a Code of Conduct on Countering Illegal Hate Speech Online, to prevent and counter the spread of illegal hate speech online.[198] The Code provides the voluntary measures that signatories can implement, such as:

- introducing in their terms and conditions a prohibition against the promotion of incitement to violence and hateful conduct;
- adopting clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content and provide information on the procedures for submitting notices;
- reviewing the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content;
- encouraging the provision of notices and flagging of content that promotes incitement to violence and hateful conduct at scale by experts and making information about 'trusted reporters' available on their websites;
- providing regular training to their staff on current societal developments, exchanging views on the potential for further improvement and identifying and promoting independent counter-narratives, new ideas and initiatives, and supporting educational programs that encourage critical thinking.

6.5.1 Discussion

Report on the Code of Conduct on Countering Illegal Hate Speech Online. The implementation of the Code of Conduct is evaluated through a regular monitoring exercise set up in collaboration with a network of organisations located in the different EU countries.

In June 2020 the European Commission published the firth report on the implementation of Code.[199] The results are as follows:

- The evaluation of the Code of Conduct on Countering Illegal Hate Speech Online shows that the Code continues to deliver positive results. On average 90% of the notifications are reviewed within 24 hours and 71% of the reported content is removed;
- Removal rates varied depending on the severity of hateful content. On average, 83.5% of content calling for murder or violence of specific groups was removed, while that using defamatory words or pictures to name certain groups was removed in 57.8% of the cases;

[196] See Décision n° 2020-801 DC du 18 juin 2020, available at https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm.

[197] The Code was originally signed by Facebook, Microsoft, Twitter and YouTube on a Code of Conduct on Countering Illegal Hate Speech Online, and later by other companies, such as Instagram, Google+, Snapchat, Dailymotion and Jeuxvideo.com.

[198] See The EU Code of conduct on countering illegal hate speech online 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

[199] See European Commission (2020). Factsheet: Countering illegal hate speech online 5th evaluation of the Code of Conduct Brussels, Consumers.

- Removal rates of content reported using trusted reported channels as compared to channels available to all users was higher. However, the report does not mention how the removed content is apportioned, distinguishing between that calling for murder and violence, that related to the use of defamatory words, and other content;
- Most of the IT companies must improve their feedback to users' notifications.

Reports on the implementation of the NetzDG. The NetzDG imposes a reporting obligation on platforms that have more than 2 million users and which receive more than 100 requests for content removal per year. Despite their limited informative capacity (further discussed below), they show an important feature: complaints are first processed by platforms on grounds included in their community guidelines; only afterwards, if the complaint is rejected and if the user also submitted a complaint under the NetzDG provisions, it is assessed on the grounds of the NetzDG.[200]

Critical issues: (i) lack of transparency and limited efficacy of the reporting systems. The aforementioned reports and assessments show that ex ante measures to reduce hateful speech could be improved. Most importantly, despite the reporting obligations described above, there is a lack of significant information on the application of the measures adopted under both the Code of Conduct and the NetzDG. This highlights the need to formulate transparency rules more clearly, so that the data collected can serve the purpose of meaningful assessment and iteration. Indeed, the information provided by OPs on their implementation of the Code of Conduct is incomplete, as it merely focuses on the number and speed of removal, without actually explaining, for example, which percentage of the removed content was found 'illegal', and how much of it was later found to be the result of over-removal.[201] Likewise, social networks' reports on the implementation of the NetzDG do not provide the expected clarity on the way platforms handle and moderate unlawful content as they lack substantial insights. On the contrary, reports should provide clear and complete information about the nature, quantity and quality of the contested material, the procedures adopted to tackle it, the percentage of removal and the ground upon which the latter was adopted, as well as on possible mechanisms on the contestation of the removal.[202]

(ii) The 'de facto' regulatory roles by online platforms, and the effects of legal fragmentation on over-removal tendencies. Indeed, removal is often disposed on the basis of definitions of hateful or harmful speech that are unilaterally set forth by platforms themselves in their policies, which go beyond, or have no direct connection to the definitions established by the law. Absent clear and harmonised obligations, OPs have the tendency to base their policies on allowed and disallowed material on the most restrictive national legislation, with the aim to minimise the risk of fines, while at the same time avoiding to adopt different conditions and terms of use on the basis of the State where the service is provided. In some case, they consider a content 'harmful', and thus proactively remove it, according to the number of 'dislike reactions' associated with it. Yet, again, this tendency could incentivise censorship and over-removal of content, with severe implications on the users' freedom of expression.[203] This tendency is then severely exacerbated when the procedures associated to content removal do not offer sufficient safeguards: on the one hand, lack of a mechanism for appeal may leave

[200] See Heldt (2019). Reading between the lines and the numbers: an analysis of the first NetzDG reports.

[201] See de Streel, Defreyne, Jacquemin, Ledger, Michel, Innesti, Goubet and Ustowski (2020). Online Platforms' Moderation of Illegal Content Online., 31.

[202] As seen from above in European Commission (2020). Countering illegal hate speech online 5th evaluation of the Code of Conduct., the information provided refers only to the total percentage of removal and to types of content removed, without providing an index with all grounds and nature of content removed.

[203] Similarly see Baistrocchi (2003). 'Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce.' Santa Clara High Technology Law Journal 19(1): 111-130.

many instances of over-removal un-tackled, clearly affecting users' freedom of speech; on the other hand, companies' failure to provide feedback to notifications reduces the beneficial effects of having a content moderation mechanism in place, as not knowing whether the content has been removed or not may provide a sense of disempowerment, and reduce the users' knowledge and understanding of what type of content is allowed or disallowed online.

6.6 Disinformation and voting manipulation

Disinformation and its social concern. Disinformation constitutes 'false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm'.[204] Despite its harmful nature, it 'very often does not qualify as illegal content', and 'where it does qualify [as such] (e.g. as defamation or hate speech), it will also be subject to specific remedies under Union or national law (e.g., take-down of content)'.[205] In other words, disinformation in itself shall be distinguished from other (properly) illegal phenomena which are analysed in different sections (§6.7).[206]

Online disinformation is particularly dangerous, as it spreads at an increased speed and has potentially unlimited reach, and is the object of growing concern at the national and international level.[207] Indeed, OPs are often maliciously used to misinform citizens, manipulate their views and spread fake news, for example, through multiple low-level websites, private messaging apps, search engine optimisation, manipulated sound, images or video, AI, online news portals and TV stations.[208]

Voting manipulation and its social concern. Voting manipulation constitutes one of the major aims of disinformation, since misleading, false, or scurrilous news is often used to influence political discourse and elections.[209] This phenomenon includes also the diffusion of content which, despite accurate, is presented in a way that distorts people's belief and opinions, such as in the case of 'filter-bubbles' and political/ideological polarisation caused by micro-targeted content,[210] giving rise to deep-seated misinformed beliefs and causing significant harm.[211]

---

[204] See European Commission (2018). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Tackling online disinformation: a European Approach. COM(2018) 236 final Brussels, European Commission. Also see European Commission (2018). Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation. JOIN(2018) 36 final Brussels, European Commission. , p. 1: 'disinformation does not include inadvertent errors, satire and parody, or clearly identified partisan news and commentary'.

[205] See European Commission (2019). Joint Communication European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. Report on the implementation of the Action Plan Against Disinformation. JOIN(2019) 12 final Brussels, European Commission. , p. 5.

[206] See COM(2018) 236 final, p.1 and COM(2018) 794 final, p. 4.

[207] European Parliament (2019). European Parliament recommendation of 13 March 2019 concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties (2018/2115(INI)) Luxembourg. Also see Bradshaw and Howard (2018). Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation Oxford. , pp. 3 and 11 ff, where the authors show that 'in each country there is at least one political party or government agency using social media to manipulate public opinion domestically'. The report found evidence of fake accounts in 46 of the 48 countries by examining three kinds of fake accounts: (1) automated accounts; (2) human accounts; and (3) hybrid or cyborg accounts. It also found evidence of formally organised social media manipulation campaigns in 48 countries, up from 28 countries in 2017.

[208] See COM(2018) 236 final,p. 5; European Parliament (2019). European Parliament Recommendation (2018/2115(INI)); European Data Protection Supervisor (2018). Opinion 3/2018 on online manipulation and personal data. pp. 5-6.

[209] See European Data Protection Supervisor (2018). Opinion 3/2018 on online manipulation and personal data., p. 3

[210] See ibid., p. 7.

[211] See High level Group (2018). A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation Belgium, Directorate-General for Communication Networks. , p. 12.

Complexity of the phenomena. Both disinformation and voting manipulation constitute 'problems of many hands', as they involve both advertisers, online platforms, non-commercial organisations (i.e. political parties) and platforms' users alike. Therefore, many strands of action are required to tackle disinformation and voting manipulation both together and separately, such as by promoting enforcing measures, and educational and transparency-related measures. In this sense, the legal landscape that we are going to discuss so far is also complemented by rules on commercial advertising set in the AVMSD, which specifically require VSPS providers to ensure the transparent nature of advertising, as to be distinguished from editorial content (see section 6.2). Likewise, since disinformation is often connected to the solicited or unsolicited creation of personalised content, the rules on collection and processing of personal data, as well as on the privacy of communications and cookies-placement set out, respectively, in the GDPR[212] and the ePrivacy Directive (see section 6.10),[213] have an important role in shaping that issue. However, in as much as they do not directly relate to the fight against disinformation, they will not be directly analysed in this section.

EU Policy initiatives. The Commission's Communication on Tackling Online Disinformation. The EU has made extensive efforts to tackle disinformation and voting manipulation. Following *inter alia* the scandal of the interference with the UK and US elections, in its Resolution on online platforms and the digital single market,[214] the EU Parliament solicited the Commission for action. The latter set up a high-level expert group and a public consultation,[215] and in April 2018 released a Communication on Tackling online disinformation,[216] where it calls on Member States to put forward several tools to tackle the spread and impact of online disinformation and ensure the protection of EU values and democratic systems. In particular, these tools shall ensure diversity and credibility of information, as well as transparency over the way it is produced or sponsored, and strive for inclusive solutions with broad stakeholder involvement. In particular, the Commission urged OPs to act swiftly and effectively to protect users from disinformation and to create a more transparent, trustworthy and accountable online ecosystem.[217]

Following this line, the European Union has outlined an Action Plan to strengthen cooperation between Member States by (i) improving detection, analysis and exposure of disinformation; (ii) ensuring stronger cooperation and joint responses to threats; (iii) enhancing collaboration with OPs and industry to tackle disinformation, (iv) raising awareness and improve societal resilience.[218]

---

[212] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

[213] See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

[214] See European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI)).

[215] See Synopsis Report of the European Commission of 26 April 2018 of the public consultation on fake news and online disinformation, available at: https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-fake-news-and-online-disinformation. Also see Flash Eurobarometer 464 (2018). Report on fake news and disinformation online, Directorate-General for Communications Networks. For further research on the matter, please see de Streel, Defreyne, Jacquemin, Ledger, Michel, Innesti, Goubet and Ustowski (2020). Online Platforms' Moderation of Illegal Content Online., pp. 34 ff; Marsden and Meyer (2019). Regulating disinformation with artificial intelligence Brussels, Service, Marsden, Meyer and Brown (2020). 'Platform values and democratic elections: How can the law regulate digital disinformation?' Computer Law & Security Review 36; Lazer, Baum, Benkler, Berinsky, Greenhill, Menczer, Metzger, Nyhan, Pennycook, Rothschild, Schudson, Sloman, Sunstein, Thorson, Watts and Zittrain (2018). 'The science of fake news. Addressing fake news requires a multidisciplinary effort.' Social Science **359**(6380): 1094-1096.

[216] See COM(2018) 236 final. Also see JOIN(2018)36 final.

[217] See ibid., p. 8. Also see COM(2018) 794 final.

[218] See COM(2018) 236 final.

Self-regulation. The Code of Practice on Disinformation. Urged by the Commission's call to develop an EU-based Code of Practice, representatives of OPs, leading social networks, advertisers and advertising industry agreed on a self-regulatory Code of Practice to address the spread of online disinformation and fake news.[219] Under the Code, the signatories committed to four main goals:

- *scrutiny of ad-placements, political and 'issue-based' advertising*, to: (i) disrupt advertising and monetisation incentives for relevant behaviours; (ii) ensure that advertisements are clearly distinguishable from editorial content; (iii) enable public disclosure of political advertising; (iv) use reasonable efforts towards devising approaches to publicly disclose 'issue-based advertising';
- *integrity of services*, by: (i) putting in place clear policies regarding identity and the misuse of automated bots; (ii) putting in place policies on what constitutes impermissible use of automated systems, and making this policy publicly available on the platform and accessible to EU users;
- *empowering users*, by: (i) helping people make informed decisions when they encounter online news that may be false, including by supporting efforts to develop and implement effective indicators of trustworthiness in collaboration with the news ecosystem; (ii) investing in technological means to prioritise relevant, authentic and authoritative information; (iii) investing in features and tools to make it easier to find diverse perspectives; (iv) support efforts aimed at improving critical thinking and digital media literacy; (v) encouraging market uptake of tools that help consumers understand why they are seeing particular advertisements;
- *empowering the research community*, by: (i) supporting good faith independent efforts to track and research disinformation and political advertising, including the independent network of fact-checkers facilitated by the European Commission;[220] (ii) convening an annual event to foster discussions within academia, the fact-checking community and members of the value chain.[221]

The entire range of commitments does not apply to all signatories, who shall rather identify those that correspond to the product and service they offer and/or their technical capabilities. Also, the measures for implementation are to be decided by the signatories and declared and explained in annual reports publicly available.

National regulations. (i) France. Efforts in combatting disinformation and voting manipulation were also made at the national level, and France passed in November 2018 a new law against manipulation of information,[222] which imposes on OPs specific obligations during the electoral process. In particular, platforms are required to: (i) provide users with fair, clear and transparent information allowing the identification of the person/entity that pays the platform for promoting certain content, and the use of their personal data in the context of promoting information content related to a public interest debate; (ii) implement measures to combat the dissemination of false information that could disturb public order or impair sincerity, such as a mechanism easily accessible and visible that allows users to report such information, especially when it comes from content promoted on behalf of a third party, and

[219] See (2018). EU Code of Practice on Disinformation. With regards to the online platforms signatories, Facebook, Google, Twitter and Mozilla subscribed to the Code on October 2018, Microsoft on May 2019 and TikTok in June 2020. See https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[220] For the limited effects of fact-checkers in deterring/reducing disinformation, please see Lazer, Baum, Benkler, Berinsky, Greenhill, Menczer, Metzger, Nyhan, Pennycook, Rothschild, Schudson, Sloman, Sunstein, Thorson, Watts and Zittrain (2018). The science of fake news.

[221] See (2018). Code of Practice on Disinformation., pp. 4-8.

[222] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information available at https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000037151987/.

complementary measures such as transparency of their algorithms, informing the users on the origin, nature and modalities to distribute content; (iii) publish aggregated statistics on the algorithms' functions, in case of algorithms-based promotion of content related to a debate of general interest, such as recommendation, ranking or referral of information. In case of violation of said duties, online platforms may face pecuniary sanctions (a fine of EUR 75,000), as well an interdiction to exercise the activity related to the crime. With specific reference to voting manipulation, the law prescribes that when inaccurate or misleading allegations or imputations of a fact likely to alter the sincerity of the election are deliberately, artificially or automated and massively disseminated through online public communication service, the judge may, take any proportionate and necessary measures to stop this dissemination.

(ii) Germany. Germany passed on 1 October 2017 a law against fake news and hate crimes in social networks [223] - i.e. the Network Enforcement Act, also known as NetzDG –, which obliged social networks to remove manifestly unlawful content within 24 hours since receiving the complaint, although a longer period for blocking or deletion can be agreed individually with the competent law enforcement authority, and to remove or block access to other unlawful content without delay and generally within seven days. Moreover, the social network shall monitor the established procedure via monthly checks and offer training courses and support programmes delivered in the German language on a regular basis to the persons tasked with the processing of complaints. Moreover, providers of social networks which receive more than 100 complaints per year for allegedly unlawful content shall produce every 6 months reports on the handling of complaints, and publish them in the Federal Gazette and on their own website. [224] Sanctions are with fines of up to 5 million EUR.

6.6.1 Discussion

Implementation of the Action Plan Against Disinformation and the EU's policy response to the problem of disinformation. The report on the Action Plan Against Disinformation[225] shows that positive improvements were reached in the fight against disinformation, with particular reference to the scrutiny of ad placements to limit malicious click-bait practices, the reduction of advertising revenues for those posting disinformation, and the level of transparency for political ads. However, the report also highlights that more still needs to be done. In particular, the Code of Practice, in itself, has limited capacity to shape OPs' conducts and practices, as compliance is voluntary and the only sanction provided under the Code of Practice is withdrawal from the initiative. These views were also shared by the European Parliament, which in the wake of European elections called on the Commission to evaluate possible legislative and non-legislative actions which can result in the intervention by social media platforms to systematically label content shared by bots, reviewing algorithms to make them as unbiased as possible, and closing down accounts of persons engaging in illegal activities aimed at the disruption of democratic processes or at instigating hate speech, while not compromising on freedom of expression. [226]

Critical issues. (i) Limited efficacy of self-regulation. Therefore, while voluntary and self-regulatory measure may have a beneficial outcome and provide an improvement in the tackling of online disinformation, their efficiency appears limited. Absent any legal sanctions, the only incentives for complying with codes of practice are reputation and fear of future regulation, leading to a substantively

[223] See fn. 189.

[224] Available at available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Also, see Engels and Fuhrmann (2018). Network Enforcement Act in a nutshell

[225] See JOIN(2019) 12 final, pp. 3-5.

[226] European Parliament (2019). European Parliament resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP)). , p. 7.

fragmented landscape. For example, ahead of this year US presidential election, certain major platforms elected to ban political advertisements long before the elections, while others did not.[227]

(ii) Difficulty in identifying content qualifying as disinformation and risks connected to the imposition of monitoring obligations. If the approach adopted so far is not fully satisfactory, it is important to highlight that alternative and more drastic solutions, such as the adoption of general monitoring obligations, may have serious drawbacks. Indeed, while important harmonised and mandatory duties of transparency can be set to ensure that users can spot and carefully assess misleading or untrue information, an actual filtering or detection activity based on the substantive content displayed may prove problematic, as it would require an objective assessment of the truthfulness of the information displayed. While NTD systems can offer useful tools for the job, especially if carried out by independent fact-checkers and trusted flaggers, ex ante filtering and monitoring made by automatic mechanisms, with limited capacity to put the content into context, may lead to an undesirable compression of users' fundamental freedoms and rights, such as freedom of expression.

6.7 Extremist/terrorist content

Extremist/terrorist content. The risks and problems connected to the spread of terrorist content online have been long acknowledged.[228] Indeed, the ubiquity of the internet and OPs' capacity to reach a large audience and host and share content at minimal costs have attracted terrorists and criminals who want to misuse both large social media platforms, and smaller providers offering different types of hosting services globally for illegal purposes and 'to groom and recruit supporters, to prepare and facilitate terrorist activity, to glorify in their atrocities and urge others to follow suit and instil fear in the general public'.[229] Moreover, recent terrorist attacks on EU soil have demonstrated that certain ill-intended users substantially use OPs for terrorist purposes, which poses significant risks to the security of EU citizens and which may also lead to a decrease of users' trust in the internet.[230]

For these reasons, the baseline regulatory regime of the ECD has been integrated with regulatory interventions tackling this specific type of illegal content, both in terms of hard law and soft law.

Legislative framework. (i) Directive (EU) 2017/541 on combating terrorism. Directive 2017/541[231] aims to adapt EU law to fight terrorism in light of evolving threats by taking into account the international nature of terrorism and its reliance on online activities. It establishes minimum rules concerning the definitions of offences and related sanctions in this area, and introduces measures of protection, support and assistance for victims. In particular, the directive provides an exhaustive list of (i) serious offences (seriously intimidating a population; unduly compelling a government or an international organisation to perform or abstain from performing any act; seriously

[227] For reference see https://www.theguardian.com/technology/2019/oct/30/twitter-ban-political-advertising-us-election. Amid public criticism, other platforms declared that they will also take steps in this respect. See https://www.nytimes.com/2020/10/07/us/politics/facebook-will-ban-political-ads-indefinitely-after-polls-close-on-nov-3-as-alarm-rises-over-the-election.html?auth=login-google. This shows the discretionary power platforms have in deciding when and how to implement measures against voting manipulation.

[228] See European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI))., p. 10.

[229] See European Commission (2018). Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online. COM(2018) 640 final Brussels, European Commission. , p. 1.

[230] See ibid.

[231] See Directive (EU) 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 L 88, 31.3.2017, p. 6–21.

destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation) that must be considered as 'terrorist offences' when committed, or threatened to be committed for a particular terrorist aim, and extends criminal punishment to cover offences related to a terrorist group (i.e. directing such a group or knowingly participating in its activities) when committed intentionally, and (ii) offences related to terrorist activities (including, distributing online or offline a message to incite a terrorist offence). In addition to prescribing the adoption of rules on aiding and abetting, inciting and attempting, jurisdiction and prosecution, as well as penalties and sanctions for physical persons and legal entities liable for the offences, article 21 of the directive requires Member States to take measures for the prompt removal and blocking of access to online terrorist content hosted in their territory, and to obtain the removal of such content hosted outside their jurisdiction. These measures must be set by transparent procedures and provide adequate safeguards, ensuring that restrictions are necessary and proportionate, that users are informed of the reason for the restriction, and that the possibility of judicial redress is granted.

The Directive is said to be 'without prejudice to voluntary action taken by the internet industry to prevent the misuse of its services or to any support for such action by Member States, such as detecting and flagging terrorist content', which, should provide 'an adequate level of legal certainty and predictability for users and service providers and the possibility of judicial redress in accordance with national law' and 'take account of the rights of the end-users and comply with existing legal and judicial procedures and the Charter of Fundamental Rights of the European Union' (Recital 22 of Directive (EU) 2017/541).

Moreover, the Directive explicitly states that removal or blocking of terrorist or extremist content 'should be without prejudice to the rules laid down in Directive 2000/31/EC of the European Parliament and of the Council', and that 'no general obligation should be imposed on service providers to monitor the information which they transmit or store, nor to actively seek out facts or circumstances indicating illegal activity'. In this line 'hosting service providers should not be held liable as long as they do not have actual knowledge of illegal activity or information and are not aware of the facts or circumstances from which the illegal activity or information is apparent' (Recital 23).

(ii) Revised Audiovisual Media Service Directive. To complement the rules set out in the Counter-terrorism directive, Member States are now also required to ensure that VSPS adopt appropriate and specific measures to protect the general public from programmes, user-generated videos and audiovisual commercial communications containing provocation to commit a terrorist offence, as already explained in section 6.2 above.

Soft Law. The Communication and Recommendation on Tackling Illegal Content Online. Both the 2017 Communication on Tackling Illegal Content Online[232] and the 2018 Recommendation on Measures to Effectively tackle illegal content online (see Chapter 3) addressed issues of hatred, violence and terrorist propaganda, despite within the broader discussion on how to address prevention, detection and removal of illegal content online. In particular, the Recommendation suggests measures on how to reduce online terrorist propaganda, forbidding the hosting of terrorist propaganda and requiring that such content is removed within one hour after being flagged by law enforcement authorities and Europol.

(ii) Proposal for a regulation on preventing the dissemination of terrorist content online. Against this background, the EU Commission published a Proposal Regulation on preventing the dissemination of

[232] See COM(2017) 555 final.

terrorist content online.[233] Once negotiations were opened, a series of concerns were expressed by, among other, members of the United Nation Human Rights Council and by the EU Fundamental Rights Agency. An amended version of the proposal was adopted on 17 April 2019 based on the reports from IMCO and CULT.[234]

At the present stage, the proposal defines terrorist content ('material which incites or solicits the commission or contribution to the commission of terrorist offences, provides instructions for the commission of such offences or solicits the participation in activities of a terrorist group' and guides on how to produce and use explosives, firearms and other weapons for terrorist purposes), requiring that such content is removed as soon as possible and within one hour from receipt of the removal order and, most importantly, sets a duty of care for all platforms to ensure they are not misused for the dissemination of terrorist content. Furthermore, the proposal calls on platforms to take proactive measure to avoid terrorist abuse. In this line, it also prescribes the creation of mechanisms for cooperation among hosting service providers, Member States and Europol, requiring service providers and Member States to designate points of contact allowing follow up to removal orders and referrals. Finally, service providers are asked to put in place effective complaint mechanisms for content providers, and that unjustified removed content shall be reinstated as soon as possible. Likewise, Member States and platforms are asked to put in place effective judicial remedies to ensure content providers the right to challenge a removal order. In case of automated detection tools, service providers shall ensure human oversight and verification to prevent erroneous removals. As far as enforcement and compliance-checking mechanisms are concerned, the proposal sets up annual transparency reports, while service providers might face sanctions up to 4% of their global turnover if they systematically and persistently fail to abide by the legislation on terrorist content. However, no obligation to monitor or filter the content is set.[235]

Cooperative bodies and initiatives. The EU Internet Forum.[236] The EU Internet Forum is a key commitment set with the Commission's European Agenda on Security 2015, and constitutes and institutional setting where EU Interior Ministers, high-level representatives of the major OPs,[237] Europol, the EU Parliament and the EU Counter-terrorism coordinator work together with the aims to provide a framework for an efficient cooperation with the internet industry in the future, and to secure a commitment from the main actors to coordinate and scale up efforts in this area in the coming years. Against this background, the Internet Forum's goal is to prevent and fight online terrorist content, working on cooperation and exchange of information – such as the Europol's EU Internet Referral Unit, a vast database containing hashes of terrorist material removed from the Internet – and monitoring initiatives and progress in the online fight to terrorism, in particular with regards to the use and efficacy of automated flagging and removal systems.

[233] See COM(2018) 640 final.

[234] Please see https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-preventing-the-dissemination-of-terrorist-content-online.

[235] For further reference please see the Legislative Train Schedule of the action to prevent the dissemination of terrorist content online available: https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-preventing-the-dissemination-of-terrorist-content-online and the Ordinary legislative procedure 2018/0331(COD) on Preventing the dissemination of terrorist content online available at https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2018/0331(COD).

[236] The EU Internet Forum's Statutes and Bylaws are available at https://www.internetforum.eu/about/about-us.html.

[237] For a complete list of the business members, including OP, please see https://www.internetforum.eu/committee/members-area.html.

6.7.1 Discussion

Assessment of the current initiatives. While the severity of the risks associated with terrorist content online justifies a higher involvement of OPs in preventing and blocking terrorist content, the latter should not be achieved at the expenses of the respect of fundamental rights and of the rule of law – including maximum certainty, congruence, non-discrimination and enforceability.[238] Indeed, both scholars, stakeholders and independent agencies such as the European Agency for Fundamental Rights fear that the requirement of proactive measures could ultimately lead to an infringement of users' fundamental rights, especially if not complemented with a series of substantial and procedural safeguards.[239]

In particular, the following suggestions should be taken into consideration:

- increased foreseeability and clarity of the very definition of 'terrorist content online', in respect of both the type of communication involved (e.g. content disseminated in the public, rather than in private communications for personal storage) and the possibility to exclude certain forms of expression;
- provision of adequate safeguards for fundamental rights through effective judicial supervision, with the involvement of host courts and authorities in cross-border removal;
- provision of adequate safeguards against excessive limitations to the freedom to conduct a business and on the host services remedies against decisions imposing additional proactive measures;
- differentiation of prevention and removal duties based on the type and size of the OPs involved;
- more flexible deadlines for blocking and removal.

Critical issues. Need for safeguard against infringement of users' fundamental rights and freedoms. The severity of the risk posed by terrorist content and propaganda justifies the need to ensure stronger involvement of OPs in preventing and removing/blocking terrorist and extremist material, as fostered by soft law instruments, and forms of self or collaborative regulations. While particular efforts are certainly needed in the cooperation between OPs and national/European enforcement authorities, the direct involvement of OPs in moderating users-uploaded content has been pictured as problematic. However, in light of previous considerations, it is important to highlight that burdening OPs with liabilities and high sanctions against the diffusion of extremist content of their services, raises serious risks of over-detection and over-removal, possibly leading to an unacceptable restriction of users' rights and freedoms.

6.8 Unsafe Products

Product safety and product liability. Under the EU acquis, the product safety and liability regime is configured by both general provisions – most importantly the Product Liability Directive (PLD) and the General Product Safety Directive (GPSD) – as well as sectoral regulation, for example in the field of pharmaceutical products, toys, and food-related products.[240] The product safety framework ensures

[238] Similarly see European Union Agency for Fundamental Rights (2019). FRA Opinion – 2/2019 Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications Vienna. and van Hoboken, Quintais, Poort and van Eijk (2018). Hosting Intermediary Services and Illegal Content Online.

[239] See European Union Agency for Fundamental Rights (2019). FRA Opinion – 2/2019 Online terrorist content.

[240] The general provisions are comprised of the Product Liability Directive (Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for

that products traded onto the EU market are safe, and continue to be so during their entire life-cycle, with mandatory specifications and procedures guiding producers in the manufacturing and commercialisation phase and establishing specific sanctions in case of non-compliance. On the contrary, product liability addresses the separate question of whom shall pay, how much, and under which conditions, if a product causes damages, even if the commercialisation of the latter was allowed under product safety rules. However, under the existing framework, limited indication is given regarding the extent to which duties and liabilities connected to the product safety and liability legislation are applicable to OPs.[241]

Product liability. The PLD[242] harmonises national product liability rules, and aims at balancing the need of not hindering socially economic activities and technological progress, with that of granting a fair allocation of the risks and costs arising therefrom, through rules that ensure safe products and adequate compensation.[243] Indeed, under the PLD 'the producer shall be liable for damage caused by a defect in his product' – i.e. when the latter does not offer the safety that a person is entitled to expect, considering all circumstances, including the presentation of the product, its reasonably expected use, and the time in which it was put into circulation (Article 6 PLD) – and liability will indeed be established upon evidence of the damage, the defect, and the causal nexus between the two (Article 1).

For the sake of this study, it is necessary to highlight that OPs may be held liable under the PLD, whenever they qualify as 'producers' according to the definitions under Article 3, namely if they are 'the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer'. This happens, for instance, with marketplaces selling products manufactured by them as VIC.

Likewise, OPs may, under certain circumstances, qualify as 'importers of products from outside the EU', or 'suppliers', thus being subject to liability whenever the producer may not be identified, unless they inform the injured person, within a reasonable time, of the identity of the producer or of the person who supplied the product. However, no clarification on the matter was provided neither in official documents, neither in the CJEU's case law, and it is doubtful whether OPs could be considered 'suppliers' for the sake of PLD when they act as 'mere intermediaries', by simply putting users in contact

defective products, OJ L 210, 7.8.1985, p. 29–33) and the General Product Safety Directive (Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2002, p. 4–17).

[241] These Directives were adopted more than 20 years ago when the risks born out of the rise of the internet and online platforms were not current, and indeed make no reference to online platforms. The European Commission launched in June 2020 an initiative to revise the General Product Safety Directive. The initiative should, among others, 'address product safety challenges in the online sales channels', possibly by 'adding requirements for online marketplaces by making legally binding some provisions of the voluntary Product Safety Pledge'. As stated under the Inception Impact Assessment 'the increasing market share of online selling (in 2018, 69% of internet users in the EU made online purchases) creates new challenges. Member State authorities do not have sufficiently effective instruments for online market surveillance (e.g. powers to acquire product samples under covert identity). New online business models and actors (such as platforms hosting third party sellers) have become prevalent, and the product safety rules for these economic operators are unclear. This affects consumer protection and creates an uneven level playing field between economic operators selling offline and online. Several online marketplaces have signed voluntary commitments to improve the safety of products online, e.g. to react within two days when a government informs about an unsafe product on the platform. As these commitments are voluntary and many economic operators do not join, safety concerns are not effectively addressed and competition between economic operators may be affected. Finally, consumers purchase products directly from operators located outside the EU more frequently, which renders it more complicated to control the safety of the product before it enters the EU market and to engage with the trader in case of safety concerns, if the trader is not represented in the EU market'. See European Commission (2020). Inception Impact Assessment. Revision of Directive 2001/95/EC of the European Parliament and of the Council on general product safety. Ref. Ares(2020)3256809 Brussels, System. , p. 2.

[242] For an overview of the directive and its implementation among Member States, see Machnikowski, P. (2016). European Product Liability. An Analysis of the State of the Art in the Era of New Technologies. Cambridge, Intersentia.

[243] See PLD, recitals.

with each other, through the designated infrastructure, especially since the PLD itself fails to give a definition of 'supplier'.

Market surveillance. While no specific obligations of monitoring or surveillance on the products placed on the platforms arise from extant regulation, the Market Surveillance Regulation[244] provides that information society services providers[245] have an obligation to:

cooperate with the market surveillance authorities, at their request;
facilitate, in specific cases, any action taken to eliminate the risks presented by a product offered for sale online through their services, or, if that is not possible,
mitigate such risks.[246]

All the aforementioned obligations are triggered by a precedent an act or measure imposed by market surveillance authorities or any other authorities. The thresholds and specific means for complying with said obligations are not outlined in the Regulation and their interpretation will be most likely further clarified through case-law and guidelines issued by the Commission under Article 33 of the Regulation or by national authorities. The Regulation also provides that the market surveillance authorities may, as a last resort,[247] request ISSPs to:

remove 'content referring to the related products from an online interface or to require the explicit display of a warning to end-users when they access an online interface'; or, where such request has not been complied with, restrict access to the online interface, including by requesting a relevant third party to implement such measures.[248]
However, these measures may be imposed only 'where duly justified and proportionate and where there are no other means available to prevent or mitigate such harm, including, where necessary, requiring the removal of content from the online interface or the display of a warning', and provided such a request is not observed by the online interface.[249] These measures consecrate at EU level the so-

[244] See Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ L 169, 25.6.2019, p. 1–44. The Regulation lays down rules and procedures for economic operators regarding products subject to certain Union harmonisation legislation listed in Annex 1 of the Regulation and establishes a framework for cooperation between economic operators, market surveillance authorities and other authorities.

[245] As per Art. 3 (14) Regulation (EU) 2019/1020 whereby 'information society service provider' means a provider of a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council'.

[246] See Art. 7 (2) of Regulation (EU) 2019/1020. Also see Recital 16: 'The development of e-commerce is also due, to a great extent, to the proliferation of information society service providers, usually through platforms and for remuneration, which offer intermediary services by storing third party content, without exercising control over that content, and therefore not acting on behalf of an economic operator. Removal of content regarding non-compliant products or, where this is not feasible, restricting access to non-compliant products offered through their services should be without prejudice to the rules laid down in Directive 2000/31/EC of the European Parliament and of the Council. In particular, no general obligation should be imposed on information society service providers to monitor the information which they transmit or store, nor should a general obligation be imposed upon them to actively seek facts or circumstances indicating illegal activity. Furthermore, hosting service providers should not be held liable as long as they do not have actual knowledge of illegal activity or information and are not aware of the facts or circumstances from which the illegal activity or information is apparent'.

[247] See Recital 41 of Regulation (EU) 2019/1020 whereby: 'in the digital environment in particular, market surveillance authorities should be able to bring non-compliance to an end quickly and effectively, notably where the economic operator selling the product conceals its identity or relocates within the Union or to a third country in order to avoid enforcement. In cases where there is a risk of serious and irreparable harm to end users due to non-compliance, market surveillance authorities should be able to take measures, where duly justified and proportionate and where there are no other means available to prevent or mitigate such harm, including, where necessary, requiring the removal of content from the online interface or the display of a warning. When such a request is not observed, the relevant authority should have the power to require information society service providers to restrict access to the online interface. These measures should be taken in accordance with the principles laid down in Directive 2000/31/EC'.

[248] See Art 14 (4) k) of Regulation (EU) 2019/1020.

[249] See Recital 41 of Regulation (EU) 2019/1020.

called notice and action procedure.[250] Most importantly, the aforementioned measures shall not conflict with the principles laid down in the ECD; in particular, no general obligation should be imposed on ISSP to monitor the information which they transmit or store, nor to actively seek facts or circumstances indicating illegal activity.[251] Yet, failure to comply with such measures will be sanctioned by the national law of the Member States and the nature of such sanctions could be administrative or penal fines for failure to comply with an administrative order. The penalties for infringement of the Regulation will be laid down in national law by the Member States.[252]

Policy and voluntary initiatives. On June 2018, four major online marketplaces signed the Product Safety Pledge[253] through the facilitation of the European Commission and thus voluntarily committed to undertake certain obligations and implement certain actions concerning consumer non-food unsafe products sold online by third parties on their marketplaces.[254] The commitments undertaken go beyond what the current EU framework legislation requires online marketplaces to do, including that on product safety.[255] They consist of:

- cooperating with the Member States' authorities by providing a single point of contact for the notification from such authorities on dangerous products, and by responding to data requests to identify the supply chain of such products;
- implementing notice and take-down procedures for dangerous products, including a clear way for customers to notify dangerous product listings;[256]
- providing sellers with information on compliance with EU product safety legislation, requiring sellers to comply with the law, and providing sellers with the link to the list of EU product safety legislation;
- implementing measures aimed at proactively removing banned product groups, preventing the reappearance of dangerous product listings already removed and acting against repeat offenders offering dangerous products;
- reporting to the European Commission the actions taken to implement the above voluntary commitments every six months.

So far, two progress reports have been published.[257] The latest report shows that the signatories have implemented measures aimed at fulfilling the voluntary commitments such as: (i) developing a Machine Learning tool which identifies and reports products that are deemed to present a high likelihood of safety concerns; (ii) developed blocking filters to proactively remove banned product groups; (iii) implemented educating campaigns for third-party sellers with respect to the applicable EU

[250] See section 5.2 of Commission Notice on the market surveillance of products sold online, C/2017/5200, OJ C 250, 1.8.2017, p. 1–19.

[251] See Recital 16 of the Regulation (EU) 2019/1020.

[252] Art 41 (1) of the Regulation (EU) 2019/1020.

[253] See (2020). Product Safety Pledge. Voluntary commitment of online marketplaces with respect to the safety of non-food consumer products sold online by third party sellers. Also see European Commission 'Product safety rules. How product safety rules are defined and enforced in the EU.' https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/product-safety-rules_en.

[254] See European Commission Product safety rules. How product safety rules are defined and enforced in the EU The Product Safety Pledge was originally signed by AliExpress, Amazon, eBay and Rakuten France. On 30th January 2020 two new online marketplaces, Allegro and Cdiscount, signed the Pledge.

[255] (2020). Product Safety Pledge., p. 1 the Pledge available at https://ec.europa.eu/info/sites/info/files/voluntary_commitment_document_2020_2signatures_v2_003.pdf.

[256] In accordance with the Pledge the response time for notices from authorities shall be that of two days and for notices from consumers the response time should be five working days.

[257] See European Commission (2018). 1st Progress Report on the Implentation of the Product Safety Pledge. European Commission (2019). 2nd Progress Report on the Implentation of the Product Safety Pledge.

legislation on product safety.[258] Furthermore, the KPIs show that over 90% of the products reported by national authorities as unsafe were removed by the signatories within 2 working days, as well as over 90% of the products identified by the signatories as unsafe through monitoring of the Safety Gate have been removed within 2 working days.[259]

6.8.1 Discussion

Critical issues. (i) Lack of binding nature of the Pledge. The Pledge initiative 'is the first of its kind in the product safety area',[260] and shows promising results. However, the Pledge is not legally-binding and it does not create any liability or rights. Thus, its fulfilment is directly dependent upon the good-faith and will of the signatories on the one hand and the fear of regulation and mandatory provisions on the other hand. Furthermore, although the signatories are major online marketplaces, encouraging and promoting the adherence to the Pledge seems to be a required step in achieving 'the objective of increasing the safety of products sold online by third-party sellers through online marketplaces'.[261]

Regardless of whether the number of signatories will increase or not, the implementation of the Pledge shows that online marketplaces can step up their efforts in increasing product safety without the latter putting a too bigger strain on their businesses. The Pledge can thus be looked at as a prolific trial period/version providing a blueprint for a future piece of regulation imposing specific duties of care on OPs.

(ii) Limited liability of OPs in their role as intermediaries. With respect to the liability of online platforms, it was stated above that some OPs, such as marketplaces, may possibly fall under Article 3 (3) of the PLD, and thus be held liable when the identity of the third-party seller acting also as a producer or importer cannot be identified. However, no indications in this sense have yet been made neither in the PLD's assessments documents nor in the CJEU's case law. If this were the case, the product liability would constitute one area of harmonised secondary liability, in contrast with (*rectius*, having special and prevalent application against) the safe harbour regime under Article 14 ECD.

A comparative perspective on OPs' liability in their role as intermediaries. Indeed, two recent cases decided in the US against a major online marketplace show that where the consumer is left with no remedies, given that the seller may not be identified, the OPs' liability could prove a viable solution.

In OBERDORF v. Amazon,[262] the United States Court of Appeals for the Third Circuit deemed Amazon a 'seller' and held it strictly liable under Pennsylvanian law, although it merely acted as an intermediary and had neither ownership nor title over the defective product. According to the Court, the platform was the 'only member of the marketing chain available to the injured plaintiff for redress'. The court also stated that there are 'numerous cases in which neither Amazon nor the party injured by a defective product, sold by Amazon.com, were able to locate the product's third-party vendor or manufacturer'.[263] Moreover, the Court stated that 'although [the platform] does not have direct influence over the design

[258] See European Commission (2019). 2nd Progress Report on the Implentation of the Product Safety Pledge.

[259] See ibid.

[260] See ibid., p. 1.

[261] See ibid., p. 1.

[262] See Oberdorf v. Amazon.com Inc, No. 18-1041 (3d Cir. 2019) at https://www2.ca3.uscourts.gov/opinarch/181041p.pdf

[263] As discussed in Ch. 4, OPs offer a variety of different services and in some case they may act also as manufacturers, distributors or fulfilment service providers that offers warehousing, packaging, addressing and dispatching, like Amazon for example. Where OPs do not act as hosting providers but trade in their own name, 'the competent authorities always have to determine in the given case in which quality the economic operator or website is to be considered' and thus, take into account that different obligations are imposed under the Regulation and other Union legislation with respect to product compliance and safety. See Commission Notice on the market surveillance of products sold online, C/2017/5200, OJ C 250, 1.8.2017, p. 1–19.

and manufacture of third-party products, [it] exerts substantial control over third-party vendors' and 'is fully capable, in its sole discretion, of removing unsafe products from its website', and, indeed, 'imposing strict liability […] would be an incentive to do so'.[264]

Similarly, a Wisconsin court held the same platform liable in a case where a Chinese manufacturer was not subject to service of process within Wisconsin's jurisdiction.[265] Here, the court stated that, by being an integral part of the distribution chain, the platform is 'well-positioned to allocate the risks of defective products to the participants in the chain' and, thus, 'bears responsibility for putting the defective product into the stream of commerce' under its jurisdiction'.

To conclude, although there is no case-law at the CJEU level on whether online platforms are deemed producers for the purpose of the PLD, such an interpretation and applicability of the PLD is recommended when the actual producer cannot be identified, as similarly seen in existing international case-law. Large online marketplaces play a substantial role in the distribution chain as intermediaries, since they usually establish the contractual terms and conditions, have the right to suspend, prohibit, or remove product listings, provide communication channels between their users, process orders and payments, etc. Thus, they exert control over how the transaction is concluded, and, if held strictly liable for damages caused by a defective product sold by their users, they may still be capable of ensuring a 'fair apportionment of the risks' in the distribution chain.[266] Furthermore, the Commission could consider extending the liability of intermediaries by adding certain duties of care to ensure that consumers have viable redress mechanisms and that compensation can be obtained alternatively from the producer, manufacturer, distributor, importer or the online platform. Additionally, obligations related to verification of third-party sellers being in good standing under the laws of the country in which they are registered and related to the thorough identification of their third-party sellers, could be imposed on OPs.

Market surveillance and Safe Harbour. As for the MSR, the provisions set therein are without prejudice to the applicability of the exception of liability laid down in the ECD, and the Commission clearly stated that the exemption from liability under Article 14 applies also 'in cases where unsafe and/or non-compliant products are sold through an online intermediary service provider'.[267] Yet, the measures imposed by the authorities under Article 14 (4) k of the Regulation can serve as a notice under Article 14 of the ECD, which may render the exemption of liability inapplicable. At the same time, if broadly framed, such measures may be deemed incompatible with the prohibition on general monitoring obligations under Article 15 ECD.

6.9 Other forms of liability: Contractual Liability

Regulating OPs' contractual relationships. OPs' relationships with their users are regulated by platforms' own Terms of Services, which reflect and at the same time are shaped by their business strategy and infrastructure, as well as by the regulatory frameworks applicable to their operations, and to the contractual agreement itself. In this sense, OPs' contract regulation resembles a 'regulatory patchwork', as it is affected by, and changes according to: (i) the European and national law in force in the Member States where the platforms offer their services (e.g., the German rules resulting from the combined application of the AVMSD and the NetzDG legislation, as far as moderation of hate speech is

[264] See Oberdorf v. Amazon.com Inc, No. 18-1041 (3d Cir. 2019), p. 14 at https://www2.ca3.uscourts.gov/opinarch/181041p.pdf, p. 16.

[265] See State Farm Fire and Casualty Company v. Amazon.com, Inc., 2019 WL 3304887 (W.D. Wis. July 23, 2019) available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3002&context=historical.

[266] See Recital 2 of the PLD.

[267] See Commission Notice on the market surveillance of products sold online, C/2017/5200, OJ C 250, 1.8.2017, p. 1–19.

concerned – see section 6.5), (ii) the applicable laws and rules on jurisdiction elected by platforms in the exercise of their contractual freedom, which, however, cannot waive mandatory EU rules or those having extra-territorial reach (Article 3 GDPR); and (iii) the specific conditions on the use of the services provided by the platforms themselves.

Although a full analysis of the rules governing OPs contracts would fall outside the scope of this study – which deals with OPs' liability for illegal/harmful content online –, a brief account of some major issues still deserves to be made, as consumer law may, under certain circumstances, constitute a ground of liability for OPs.

A first, major distinction shall be made on the different type of contracts entered into by the OPs and their users. Indeed, in some cases the interactions of the different sides of the market with the platforms give rise to two different contracts, namely: (i) the one between the platforms and each of its users, for the provision of its 'intermediation services', and (ii) another one, made by the platforms' users among themselves, directly on the platform or outside its infrastructure, and which is enabled by said intermediation.

6.9.1 Regulation of the contract for the provision of the intermediation services

Application of consumer law. When OPs offer their intermediation services to consumers, the former qualify as 'businesses' or 'professionals' and are thus directly and primarily subject to specific obligations set out in consumer law.[268] Indeed, whenever services or goods are offered to EU consumers, the application of those rules is mandatory under the Rome I Regulation,[269] and cannot be waived by the OPs' 'Terms of services', even when they establish the application of non-European law or jurisdiction.

Regulation 2019/1150 and the need for specific protection of business-user in the platform economy. Online platforms boost innovation and productivity, offering significant benefits for the businesses which their services are provided to, in terms of faster and easier circulation of ideas, products and services, sharing and allocation of resources, as well as easier, wider, and better-targeted access to audience, all thanks to the intermediation offered by the platforms, and to the advertising services connected to it. However, the peculiarities of the online-platform business model, the interdependency caused therefrom, as well as the dominance of certain platforms in their specific sector, raise issues connected to the protection of platforms' business users.[270] In particular, protection is needed against possible unfair contractual and trading practices, due to informational asymmetries as well as imbalances in the respective economic and contractual power, since said practices may lead, for example, to the removal of products or services without due notice and/or possibility to contest the decision, and to the discriminatory treatment in favour of the platforms' own products and services,

[268] Consumer law consists of a large variety of dispositions aimed at protecting consumers, with both general application and sector-specific relevance. See Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, p. 22–39, and Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29–34. Directive 93/13/EEC protects consumers in the EU from unfair terms and conditions which might be included in a standard contract for the goods and services they purchase. It introduces the notion of 'good faith' to avoid any significant imbalance in mutual rights and obligations.

[269] See Art. 6(2) under Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008, p. 6–16.

[270] OECD (2019). An Introduction to Online Platforms., p. 28 ff.

which raise public concerns, as evidence by the Commission investigation against Google for its preferential display of its own shopping services on the top of the search results page.[271]

To address these issues, the EU has adopted a Regulation specifically dealing with the promotion of fairness and transparency for the business users of online intermediation services.[272] The regulation aims to ensure that business-users are treated in a fair and transparent way by OPs, and that they have effective tools for redress when issues occur, with the ultimate aim of enabling a positive regulatory environment for the development of OPs within the EU.[273] In as much as said regulation does not directly affect the liability of OPs for the illegal/harmful online content carried out by users through the platform's infrastructure, a comprehensive account of the two would fall outside the scope of this study and then it shall suffice to refer to Annex 3.

6.9.2 Regulation of the contract for the provision of the service enabled by the platform's intermediation.

Different types of interactions. (i) Platforms as a direct contractual party. As discussed in Chapter 4, OPs adopt different business models and, thus, their users may have different types of relationships with the OPs and among themselves. This is true even within one relatively narrow type of platforms known as 'transaction platforms'.

In some cases, platforms directly engage into transactions with consumers – e.g. when acting as resellers or VIC – and said transactions are thus directly and primarily addressed by consumer protection obligations, even for the regulation of the underlying service offered.[274]

On this issue, the 2016 Guidance on the unfair contractual practice directive[275] specifically states that the platform providers could be considered 'sellers' under the directive 'if they act for purposes relating to their own business and as the direct contractual partner of the consumer for the sale of goods', or of the 'supply of digital content or digital service', and that Member States are free to extend its application to platform providers that do not fulfil these requirements (recitals 18 and 23), thus possibly leading to a fragmented landscape on this matter.

(ii) Platforms as 'mere' intermediaries. In other cases, OPs do not feature as part of the contract, as they simply put users in contact with third-party distributors or merely provide the digital environment for facilitating the exchange. In this case, it is important to consider how consumer protection affects

[271] See Summary of Commission decision of 27 June 2017 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case AT.39740 — Google Search (Shopping)) (notified under document number C(2017) 4444), OJ C 9, 12.1.2018, p. 11–14. With respect to price discrimination as a form of abusive dominance, please see Botta and Wiedemann (2019). To discriminate or not to discriminate?

[272] See Regulation (EU) 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, PE/56/2019/REV/1, OJ L 186, 11.7.2019, p. 57–79.

[273] For a critical account of the limitation to 'business-users', which leaves unexplored the contractual protection of 'hybrid sellers or service providers' unexplored: Iamiceli (2019). 'Online Platforms and the Digital Turn in EU Contract Law: Unfair Practices, Transparency and the (pierced) Veil of Digital Immunity.' European review of contract law **15**(4): 392–420.

[274] Consumer law consists of a large variety of dispositions aimed at protecting consumers, with both general application and sector-specific relevance. See Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, p. 22–39, and Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29–34. Directive 93/13/EEC protects consumers in the EU from unfair terms and conditions which might be included in a standard contract for goods and services they purchase. It introduces the notion of 'good faith' to avoid any significant imbalance in mutual rights and obligations.

[275] See European Commission (2016). Commission Staff Working Document Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices. SWD(2016) 163 final Brussels, European Commission. , p. 110-111.

the relationships entered into by platforms users among themselves, where the platforms do not act as an intermediary, reseller or representative, but merely provide the digital environment for facilitating the exchange.[276] Indeed, three different scenarios occur:

- if one of the users is a trader (B2C), EU consumer law applies;
- if both users are consumers (C2C or peer to peer), EU consumer protection law does not apply, and the transactions are merely regulated by the OPs' terms of services and national rules, which may have a general nature, or provide – upon their own basis – some extended protection to the vulnerable party.
- if the qualification of the parties is not clear cut, doubts arise whether users may be deemed acting in their personal capacity or have some level of professionalism, which would call for consumer protection rules to apply to a certain extent.

On the last issues, the Commission's Communication giving legal and policy making guidance for the Collaborative Economy sector,[277] stated that EU consumer law applies to any collaborative platform that qualifies as trader engaging in commercial practices with a consumer, and the same goes for the B2C relationships established directly between platform's users, and not apply to peer-to-peer relations.[278] Thus, it stated that clear and common criteria are required to assess whether users qualify as consumers or business, whereas the actual assessment can only be done on a case-by-case basis. Drawing from national experience and from the Commission Guidance on the UCPD, the Communication argued that Member States shall seek a balanced approach to ensure a high level of consumer protection, while not imposing disproportionate burdens on individuals who provide services without qualifying as traders; such assessment shall be based, inter alia, on the frequency of the services provided, the profit-seeking motive and the level of turnover. Finally, it highlighted how trust-building mechanisms shall be used as much as possible for the purpose of ensuring consumer protection, also as an alternative to legislative interventions.

(iii) Platforms as gatekeepers. Against this background, it is unclear to what extent platforms may be held responsible to ensure a correct regulatory environment for the relationships entered into by their users, triggering specific forms of liability. Indeed, the Commission Guidance on the application of Directive 2005/29/EC, states that, 'as regards third party economic operators acting on a platform, the platform itself should take appropriate measures to enable third-party traders to comply with EU consumer and marketing law in conjunction with EU product legislation and/or product safety law requirements (including the indication on its website of CE markings, any required warnings, information and labels in accordance with the applicable legislation)'.[279] However, the Guidance is not in itself legally binding, and does not give detailed indications on the OPs' actual responsibility on the matter.

[276] However, the platforms' level of control can vary. Please see Hausemer, Rzepecka, Dragulin, Vitiello, Rabuel, Nunu, Rodriguez Diaz, Psaila, Fiorentini, Gysen, Meeusen, Quaschning, Dunne, Grinevich, Huber and Baines (2017). Consumer issues in online peer-to-peer platform markets., p. 54 ff.

[277] COM(2016) 356 final.

[278] For an overview of the regulatory elements in P2P platform practice, please see Hausemer, Rzepecka, Dragulin, Vitiello, Rabuel, Nunu, Rodriguez Diaz, Psaila, Fiorentini, Gysen, Meeusen, Quaschning, Dunne, Grinevich, Huber and Baines (2017). Consumer issues in online peer-to-peer platform markets., p. 100 ff. On the role of consumer law in Busch, Schulte-Nölke, Wiewiórowska-Domagalska and Fryderyk (2016). The Rise of the Platform Economy.;Busch (2016). Crowdsourcing Consumer Confidence: How to Regulate Online Rating and Review Systems in the Collaborative Economy. European Contract Law and the Digital Single Market: Implications of the Digital Revolution. De Franceschi. Cambridge, Intersentia: 223-243.

[279] See Commission Notice on the market surveillance of products sold online, C/2017/5200, OJ C 250, 1.8.2017, p. 1–19.

6.9.3 Joint/Subsidiary Liability for breach of contract?

Studies addressing gaps and inconsistency in the existing legal framework. Gaps and uncertainty in the law regulating both the contract between OPs and their users, and the contracts between users concluded through the intermediation services offered by the platforms, highlighted the need for possible regulatory intervention, which has been addressed by ongoing research and policy projects, including those tackled below, namely (i) Discussion Draft Directive on Online Intermediary Platforms by the Research Group on the Law of Digital Services[280] and (ii) the ELI Model Rules on Online Platforms.[281] Indeed, these projects expressly dealt with – *inter alia* – the informational duties that OPs should be burdened with to ensure adequate users' protection, as well as with the remedies that the latter should be entitled to, whenever the contract concluded through the intermediation of the platforms is breached, which, in certain occasions, should also be directed to OPs themselves.

(i) The Discussion Draft Directive on Online Intermediary Platforms by the Research Group on the Law of Digital Services. After a series of initiatives were adopted at EU level, the Research Group on the Law of Digital Services drew up a Discussion Draft Directive on Online Intermediary Platforms,[282] which aims to provide guidance on how to regulate the contracts between the platform and the consumer and the platform and the supplier. In addition to platform's duty on its transparency, on information for customers and suppliers, the Discussion Draft Directive sets specific forms of liability of the platform operator in addition to that under platform-supplier contracts or platform-customer contracts. According to the proposal, a platform operator who presents itself to customers and suppliers as an intermediary in a prominent way is not liable for non-performance under supplier-customer contracts.[283] However, it may be liable for damages caused by misleading information presented on the platform, if the platform operator was notified about such content, and failed to take appropriate measures to remove or rectify it. Moreover, the OPs might still be held jointly liable for the non-performance if the consumer can reasonably rely on the platform influence on the supplier, as well as for damages caused to costumers because of the misleading information given about suppliers, goods, services or digital content offered by its users acting as suppliers, and for the specific warranties that it may have given on their quality.

(ii) ELI Model Rules on Online Platforms. After the Draft Directive was published, the project was taken up by the European Law Institute as a starting point for the ELI Model Rules on Online Platforms, which were developed in 2020 as a 'model for national, European and international legislators as well as a source of inspiration for self-regulation and standardisation' (Article 1.1).[284] These rules set upon

[280] See Busch, Dannemann, Schulte-Nölke, Wiewiórowska-Domagalska and Zoll (2016). Discussion Draft of a Directive on Online Intermediary Platforms.

[281] See European Law Institute (2019). Model Rules on Online Platforms.

[282] See Busch, Dannemann, Schulte-Nölke, Wiewiórowska-Domagalska and Zoll (2016). Discussion Draft of a Directive on Online Intermediary Platforms.

[283] Other than the requirement of clearly presenting itself as a mere intermediary, it is important to take into account also the platforms' actions which may create, albeit its statement as being a simple intermediary, the impression that the platform is controlling the performance of the contract. In this respect, see Hausemer, Rzepecka, Dragulin, Vitiello, Rabuel, Nunu, Rodriguez Diaz, Psaila, Fiorentini, Gysen, Meeusen, Quaschning, Dunne, Grinevich, Huber and Baines (2017). Consumer issues in online peer-to-peer platform markets., p. 129 where it is stated that: 'depending on the extent to which a platform 'intervenes' in the transactions concluded by its users, the latter may expect that the platform shares responsibility with the peers in case of non-performance or non-compliance of the performance. For example, where the platform actively manages P2P transactions (e.g. facilitating trust among peers by using or suggesting ID verification systems, managing user reviews, mediating disputes) or governs them (e.g. setting cancelation policies, providing insurance and refunds), it is more likely that its users have the impression that the platform will also share a certain degree of liability'. Also, the authors state that 'from a consumer policy perspective, greater control over the transaction implies or creates the impression of greater platform responsibility for the performance of the transaction, for pre-contractual and contractual information'.

[284] See European Law Institute (2019). Model Rules on Online Platforms.

operators of information society services[285] a series of transparency obligations concerning the conditions of the contract and the features of the service provided by platform operators (PO),[286] but explicitly exclude them from any general duty to monitor the activity of their users or the information presented by suppliers or customers, unless provided otherwise by law (artt. 8, 9). Moreover, the Model Rules suggest that OPs must clearly inform their users that they will not enter into the contract with the platform – which acts as an intermediary – but rather with the supplier, (Article 13), and give relevant information on the matter (whether it is a trader and whether consumer law applies to the contract, and its identity). However, if the PO fails to do so, then 'the customer can exercise the rights and remedies available against the supplier under the supplier-customer contract also against the platform operator)', thus holding the platform operator liable for lack of transparency (art 19). Likewise, if the customer can reasonably expect the platform operator to have a predominant influence over the supplier, the latter becomes jointly liable for the supplier's non-performance' (Article 20).[287] In both cases, the OP will be able to act in recourse against the supplier, while the latter will be able to initiate a secondary litigation against the PO, whenever the misleading statements made by the PO caused the supplier to incur any liability (Article 25). Furthermore, the PO is liable for damages arising to customers or suppliers from any misleading statement made, for the guarantees given, and for the damage caused by a violation of its primary duties (Article 24).[288]

6.10 Other forms of liability: Data protection

The use of an unprecedented volume of data, both personal and non-personal, and the capacity to use it to improve the services offered by the OPs' users, and to sell aggregated data to advertisers, constitute some of the characterising features of the digital platform economy.

Legislative framework. The General Data Protection Regulation and the e-Privacy Directive. The two major elements in this segment of the regulatory framework are the General Data Protection Regulation and the E-Privacy Directive.[289] The first one regulates the collection and processing of

[285] The ELI Model Rules on Online Platforms 'are intended to be used in relation to platforms which: (a) enable customers to conclude contracts for the supply of goods, services or digital content which suppliers within a digital environment controlled by the platform operator; (b) enable suppliers to place advertisements within said digital environment which can be browsed there to contact suppliers and to conclude a contract outside the platform; (c) offer comparison or other advisory services to customers which identify relevant suppliers of goods, services or digital content and which direct customers to those suppliers' websites or provide contact details; (d) enable users to provider reviews regarding suppliers, customers, goods, services or digital content offered by suppliers, through a reputation system'. See ibid., Art. 1(2).

[286] As indicated under 'Chapter II: General Obligations of Platform Operators Towards Platform Users' of the ELI Model Rules on Online Platforms, the PO must: provide easy accessible, clear and machine readable information and contract terms, and make the latter easily available at all times (Art. 3); provide information about the main parameters determining rankings for search queries and their relative importance must be easily accessible, and disclose if influenced by remuneration or other significant ties with suppliers (Art. 4); provide information about how the information for reputational systems is collected, processed and publishes and using ranking systems in a way that complies with the requirements of professional diligence, which is presumed in case of voluntary compliance with relevant standards or with the criteria set out in Art. 6 (Art. 5-6) ; provide facility for allowing portability of reviews and relevant information for export to and import from other platforms (Art. 7); act in good faith and fair dealing when unilaterally changing the terms of the contract, and give a reasonable notice (minimum 1 month) (Art. 12). See ibid.

[287] For this assessment, the following criteria may be considered in particular: the reliance of the supplier-customer contract on the platform facilities, stage of disclosure of the supplier's identity, use of payment systems allowing payment withholding, determination of the contract's terms and price, marketing focus and PO's statements over the monitoring of the suppliers conduct and compliance enforcement under the platforms' rule.

[288] Specifically, for those duties and guarantees set forth in Art. 3, Art. 4, Art. 5, Art. 7, Art. 9 paragraphs (2)and (3), Art. 10, Art. 11, Art. 14, Art. 16, Art. 17, Art. 18.

[289] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of

personal data, granting specific rights to data subjects and requiring a series of duties of governance and accountability to data controllers and processors. The second one establishes rules to ensure the users' right to privacy and confidentiality in the exchange of information through public electronic communication services (such as the internet and mobile/landline telephony).

Thus, the rights and duties that the entities acting within such online environments have substantially shaped the behaviour of OPs, and also shape their liability. For example, under Article 85 GDPR, OPs who qualify as controllers may be subject to an injunction by a national court or enforcement authority in case they failed to ensure access to personal data upon request of the data subject; or an order to erase it when the data subject wishes to do so, and there is no legitimate reason to keep it; or an administrative sanction in case of failure to comply with specific duties, such as the obligation to notify a breach, as well as an award for damages to compensate for harmful consequences deriving therefrom. In terms of technical infrastructure, OPs are required to comply, *inter alia*, with the principle of data-protection 'by-design and by default' and need to adopt organisational measures to ensure adequate assessment of the risks connected to the use of personal data (e.g. presence of a Data Protection Officer).

However, in as much as said regulation does not directly affect the liability of OP for the illegal/harmful online content carried out by users through the platform's infrastructure, a comprehensive account of the applicable provisions is carried out in Annex 3.

Indeed, for the sake of this study is important to recall that – since OPs have important duties under the data protection regulation – whatever form of content regulation that they may initiate, or that they may be called to perform in the future – must necessarily comply with EU and national rules in the field and, at a more general level, must be respectful of the users' fundamental rights to privacy and data protection under Article 7 and 8 under the Charter of Fundamental Rights of the European Union.

Search engines and social medial platforms as personal data controllers. Indeed, the CJUE has decided in two landmark cases on whether search engines operators and social medial platforms can be deemed as controllers under the personal data protection regulatory framework.[290] In both case, the CJEU highlighted that the notion of 'controller' shall be construed broadly. With respect to search engines operators, the CJEU stated the latter 'determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and […] must, consequently, be regarded as the 'controller'".[291] Furthermore – the Court stated – it would be contrary to the provisions' objectives defining the notion of controller — 'which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties'.[292] With respect to social media platforms, CJUE clearly held that they must be regarded as primarily determining the purposes and means of processing the personal data of their users and persons visiting the fan pages hosted on their infrastructure, and therefore fall within the concept of 'controller"'.[293]

privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.

[290] See Case C-131/12, Google Spain and Google, EU:C:2014:317 and Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388, where the CJEU analysed the notion 'controller' as defined under Art. 2 (d) of Directive 95/46, which was transplanted into Regulation 2016/679.

[291] See Case C-131/12, Google Spain and Google, EU:C:2014:317, para. 33.

[292] See Case C-131/12, Google Spain and Google, EU:C:2014:317, para. 34.

[293] See Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388, para. 30.

7. Latest policy initiatives in regulating online platforms' liability

Current discussion on a possible Digital Service Act. Following President von der Leyen's mention to the Digital Services Act in her political guidelines for the next European Commission,[294] the Commission and the European Parliament are currently discussing[295] the possibility to draft and adopt a horizontal regulatory framework for all digital services in the single market, which is supposed to address a series of issues considered of particular importance in the digital economy landscape. The regulatory status quo is deemed inadequate because:

- there are divergent rules for online services across the digital market, which cause significant regulatory fragmentation (e.g. in the field of online advertising, where Member States have started adopting their own national rules);
- many key instruments are outdated, and contribute to the emergence of a regulatory gap for modern digital services (e.g. the active/passive distinction as currently set out by the e-Commerce Directive; the lack of rules on cross-border micro-targeting political advertising);
- current rules are perceived as not incentivising prevention and prompt removal of harmful and/or illegal online content, e.g. because service providers fear that they will become liable for the intermediation, losing the exemption under the e-Commerce directive;
- public oversight is considered ineffective, ultimately leading to the delegation of regulatory powers to online platforms themselves;
- innovative services are faced with high entry barriers, with no rules enabling regulatory experimentation.

To overcome these problems, working groups within the Commission argued for the adoption of horizontal instruments – from a REFIT of the ECD, to a Digital Service Act or a Digital Service Code –, which could complement the sectoral and 'problem-based' strategy advocated by the 2016 Communication on Online Platforms. Said policy-option would:

- have an updated scope and territorial application, as it would cover the entire stack of digital services (not being limited to information society services, as it is with the ECD), thus covering ISPs, cloud services, content delivery networks, domain name services, social media services, search engines, collaborative economy platforms, online advertising services, digital services built on electronic contracts and distributed ledgers), with possible distinctions based inter alia on their market status; despite addressed to the internal market and based on the 'home state control' principles, new rules should also cover services established in third countries, where directed to EU citizens or residents';
- maintain the liability exemptions for intermediaries, but expand the current ones as to cover services other than those providing mere hosting, conduit and cashing, including those already specified in the CJEU's case law (such as search engines and wi-fi hotspot), update the active/passive distinction, and set a 'good Samaritan' rule;
- set specific rules on algorithm-based filtering, without introducing any duty of general monitoring (as in Article 15 ECD);

[294] See von der Leyen (2019). A Union that strives for more.

[295] See European Commission (2020). Inception Impact Assessment. Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services. Ref. Ares(2020)2877686 Brussels, European Parliament (2020). Digital Services Act: Improving the functioning of the Single Market European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)). TEXTS ADOPTED. Provisional edition.

- set uniform rules on the removal of illegal content, NTD rules and transparency obligations;
- pressure for the adoption of codes of conducts and user-empowerment tools to combat harmful content, which is not suitable for notice-and-take-down actions;
- regulate content advertising services;
- regulate service interoperability;
- set instruments for regulatory experimentations, public-authority oversight and cooperation.

8. Policy options

Aims and methodology of this section. This section aims to identify and critically assess a set of different policy options, which could be used to shape OPs' liability for the illegal/harmful content or products distributed and/or made available through their infrastructures, such as content infringing IP rights, hate speech, terrorist content, content that harms children, and unsafe product. While the regulatory possibilities in the field are many and highly heterogeneous, this study only focuses on feasible and realistic ones, excluding those that could be delivered only at an unacceptable timescale or cost.

For this purpose, the policy options build upon the main findings of the study regarding OPs' rights, duties and liabilities, as well as the incentives that the latter have to develop a safe online environment, in light of the different characteristic displayed by OPs, the heterogeneous types of harm caused, and the various subjects involved (section 4.3.1). In doing so, the relevant legal framework, the voluntary and self-regulatory initiatives established in the field, the practices adopted by the same actors, and the existing EU policies, including the proposals under discussion at the time of writing, were considered.[296]

The policy options are presented along a scale of increasing interventionism – from 'maintaining the status quo', to 'statutory interventions'. However, they shall not be seen as mutually exclusive. Indeed, with the only exception of the first policy option (amounting to 'no action') (see section 8.2.1), all of them can be implemented on their own, or combined with one another, whenever compatible. For example, the option of 'strengthening self-regulatory instruments' (see section 8.2.3) may be considered both as an alternative to the aforementioned extremes of the spectrum, and as one step of a multi-layered regulatory jigsaw. As such, it could interact with other tools and solutions, eventually ensuring positive synergies and mutual reinforcement strategies. Such possible positive interactions are discussed when relevant.

The policy options are assessed based on their performance against various criteria, including: cost and benefits; feasibility and effectiveness; sustainability; risks and uncertainties, as these may (i) impact the policy and its objectives; (ii) provide coherence with EU objectives; and (iii) have potential ethical, social and regulatory impacts. Specific attention is paid to their effects on EU citizens' fundamental rights and freedoms.

Each option is discussed, detailing its pros and cons. However, an in-depth analysis is reserved for those that clearly appear preferable. Moreover, within each option, a series of more granular solutions are identified and discussed.

Before moving to the analysis, however, some considerations on general and methodological concerns in the regulation of OPs shall be made.

[296] See European Commission (2020). IIA. Digital Services Act ; European Parliament (2020). Report with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)). Plenary sitting. ; Committee on Legal Affairs (2020). Opinion of the Committee on Legal Affairs for the Committee on the Internal Market and Consumer Protection with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)). ; Committee on Transport and Tourism (2020). Opinion of the Committee on Transport and Tourism for the Committee on the Internal Market and Consumer Protection with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)). ; Committee on the Internal Market and Consumer Protection (2020). Draft Report with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)). ; Lomba and Evas (2020). Digital Services Act. European added value assessment.

8.1 General considerations guiding the identification and assessment of the policy options

Liability as one component among others. The EU approach to the regulation of OPs aims to achieve the framework that best incentivises all subjects involved to prevent the diffusion of such illicit/harmful content online, to promptly remove it when diffused, and to repair the consequences deriving therefrom. The OPs' liability for third-party illegal/harmful content constitutes only **one element** of a broader regulatory framework, which could be used for the attainment of this goal. Thus, liability rules cannot be considered in isolation, but rather as specific tools that interact with other regulatory instruments, and whose role and effectiveness shall be analysed accordingly.

The functions of liability. A risk management approach. For example, liability does not need to work **in itself** as an incentive towards the adoption of specific behaviours, if the same result can be better achieved through other instruments. Indeed, in some cases, non-liability-related instruments are more suitable for incentivising OPs to adopt an optimal level of content management and moderation, while OPs' civil liability can be directed towards purposes different from deterrence. Most importantly, it can be devoted to ensuring that victims of illegal/harmful behaviours are adequately compensated. Under a risk management approach (RMA),[297] this would occur whenever platforms (i) would be in the best position to ensure prompt and full compensation, and (ii) would be able to adequately manage the risk connected to the imposition of such liability, e.g. by means of insurance, or shifting the costs back to the users who are actually responsible for the damage.

Indeed, under a RMA, ex-ante safety and security should be decoupled from ex-post compensation, leaving it to other and more effective mechanisms – such as technical regulation – to achieve desired standards of conduct. Liability shall thus be strict – if not absolute – rather than fault-based, while other tools and instruments – such as rules prescribing how the platform should be designed and function – shall be further exploited by adopting ex-ante detailed regulation and technical standards. To ensure prompt and full compensation, said strict or absolute liability shall be attributed to the platform as a single, clear and unquestionable entry point for all litigation (one-stop-shop). On its part, the platform held liable for wrongs caused by its users, could then transfer the cost to all other users (pooling and spreading effect) through insurance and price mechanisms (e.g. adjusting subscription fees), and should be allowed to exercise its right of recourse against the person who actually caused the harm. To ease management of higher risks, different approaches might be considered, including (i) compulsory third-party insurance, when statistical data allows for risk-assessment; (ii) automatic compensation funds, financed through ad hoc taxes/fees imposed on the platforms and/or their users; (iii) damage caps and limitations, proportionate to the specific risks brought about (section 5.1).[298]

Technologically-specific regulation. The principle of 'technological neutrality' is often used to argue that regulation should rely on broad definitions and general clauses to be future-proof,[299] i.e. survive technological development without the need for constant revisions.[300] On the contrary, according to a 'technology-specific approach', regulators should strive to address narrowly identified problems posed

[297] See Palmerini and Bertolini (2016). Liability and Risk Management.

[298] Bertolini (2016). Insurance and Risk Management.

[299] Koops, B.-J. (2006). Should ICT Regulation Be Technology-Neutral?. Starting Points for Ict Regulation. Deconstructing Prevalent Policy One-Liners. It & Law Series, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, eds. The Hague, T.M.C. Asser Press. 9: 77-108., 9, available at SSRN: https://ssrn.com/abstract=918746

[300] Greenberg, B. A. (2016). 'Rethinking Technology Neutrality.' Minnesota Law Review 100:1495., 1512-1513.

by specific classes of application, focusing on their social implications.[301] While the EU has long committed to a 'sector-specific' and 'problem-driven' approach in the regulation of OPs (Chapter 3) many solutions discussed in light of the announced Digital Services Act seem to go towards the adoption of transversal and horizontal rules, applicable to a broad variety of large digital services providers.[302]

While this option has some benefits, especially if thought as granting a sort of 'baseline' regulatory regime – on which other, sector-specific rules would rely – the attempt to deliver future-proof definitions and all-encompassing regulations is most likely destined to fail. Indeed, such effort would be both incomplete and ineffective, since future developments may still be hard to frame within the provided definitions, and specific concerns and opportunities may not be adequately addressed in the effort to make general rules.[303]

Thus, the preferred option would be to conceive of regulation as an evolving tool, to be modified together with technological advances through constant and attentive monitoring of emerging solutions and their specific impact on individual and social rights, as well as on the socio-economic structure of our society. Ideally, such constant monitoring could be carried out by specifically designed bodies, as suggested under section 6.1.[304] Indeed, a devoted institution could be established as the main reference point for proposing regulatory intervention, and to allow coordination and cross-fertilisation among different policies and objectives, as well as a single point of contact for national authorities and OPs across the EU.[305]

8.2 Suggested Policy Options

8.2.1 Maintaining the status quo

Description. Under this option, no action at the European level would be adopted. The regulatory framework would continue to consist of the 'Safe Harbour' for intermediary liability, complemented with sectoral legislation providing for specific duties and specific forms of liability (such as that defined by Article 17 of the new Copyright Directive, section 6.3), as well as by self-regulatory initiatives (such as the Code of Practice on Disinformation, section 6.6).

Benefits. This option would have the benefit of bearing no costs, while allowing the EU to reap the positive effects that are expected to derive from the most recent initiatives in the field, as well as from the various calls for shared responsibility in the fight against online/harmful content.[306] Moreover, it would allow OPs a wide space for experimenting with technical solutions for content detection and moderation, and for practices to evolve together with new challenges. In this sense, it would foster

[301] Bertolini, A. (2013). 'Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules.' Law Innovation and Technology 5(2): 214, Bertolini, A. and E. Palmerini (2014). Regulating Robotics: a Challenge for Europe. Upcoming Issues of EU Law, available at http://www.europarl.europa.eu/document/activities/cont/201409/20140924ATT89662/20140924ATT89662EN.pdf. D.-G. f. I. Policies. Bruxelles., 180-182.

[302] While the policy options to be followed under the DSA are still under review, please allow reference to Committee on Legal Affairs (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market. (2020/2018(INL))., advising the Commission against adopting a general duty of care.

[303] See Bertolini (2020). Artificial Intelligence and Civil Liability.

[304] See Smith (2020). Enforcement and cooperation between Member States. E-Commerce and the future Digital Services Act Luxembourg.

[305] See Sartor and Loreggia (2020). The impact of algorithms for online content filtering or moderation Brussels, Policy Department for Citizens' Rights and Constitutional Affairs. , p. 65.

[306] See COM (2016) 288 final, COM(2020) 67 final. COM(2017) 555 final, COM(2016) 356 final, C(2018) 1177 final, European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI)).

research into creating further evidence-based policies concerning the development and functioning of new OPs, based on the practices concretely adopted by the latter to manage material uploaded to their infrastructure, as well as the legislative responses that already exist.

Drawbacks. However, this option would leave many gaps and risks unaddressed that negatively impact the functioning of OPs and their capacity to increase the fight against illegal/harmful content online, identified in the study. Indeed, chances are that spontaneous practices would not solve these issues, but rather exacerbate them. In particular, the adoption of the *Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*, and the Network Enforcement Act demonstrate that legislation is likely to be adopted at the national level,[307] increasing legal and market fragmentation, and seriously hindering legal certainty over the rights, duties and liabilities of OPs, as well as of all the other subjects involved.

Recommendations. We suggest that this option should be discarded.

8.2.2 Awareness-raising, and media literacy campaigns

Description. Under this option, the EU would direct its efforts at ensuring that Member States and OPs adopt tools and instruments capable of strengthening media literacy and empowering users, to allow OP users and society at large to actively promote a safe digital environment, for example by promoting awareness-raising campaigns.

Benefits. Indeed, on many occasions this study highlights that fighting the spread of online illegal/harmful requires the involvement of many different subjects at the same time,[308] and it is essential that users of digital services have the knowledge, sensibility and actual capacity to identify and report defamatory content, fake news, or content that could be dangerous for children, to name but a few. Moreover, the initiatives undertaken under this option would have limited realisation costs, and would work in strong synergy with existing projects and campaigns. OPs should be a proactive collaboration partner in this respect, given their global reach and ability to promote and massively distribute information.

Drawbacks. However, it is important to highlight that the user protection achieved through 'empowering tools' is often sub-optimal. On the one hand, users and members of society have little incentive to control OPs through their choices or behaviour. In certain cases – such as in IP law related infringements – victims may have very high incentives to flag content shared in breach of their exclusive rights.[309] Conversely, for wrongs and dangerous content that are most likely to affect society at large, individual users have fewer incentives to take a proactive monitoring and reporting role, while NGO and consumer associations often lack the adequate resources to do so. On the other hand, imposing extensive requirements of information, awareness-raising and transparency on OPs may, in itself, not be sufficient to actually make users aware of their rights and duties. Experience in the application of data protection laws shows that users do not read privacy policies, and subsequently consent is not truly informed, while the imposition of extensive procedural informational duties may

[307] Germany passed on 1 October 2017 a law against fake news and hate crimes in social networks i.e. the Network Enforcement Act, also known as NetzDG., available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. See Engels and Fuhrmann (2018). Network Enforcement Act in a nutshell Also, in June 2020 the French Parliament adopted Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet available at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970.

[308] Helbergera, N., T. Poellc and J. Piersonb (2018). 'Governing online platforms: From contested to cooperative responsibility.' The Information Society 34(1): 1-14.

[309] See de Streel, Defreyne, Jacquemin, Ledger, Michel, Innesti, Goubet and Ustowski (2020). Online Platforms' Moderation of Illegal Content Online.

result in reducing, rather than fostering, OPs' responsibilities,[310] as they can avoid liability by proving that they met such 'formal' requirements.

Recommendation. For the aforementioned reasons, we suggest that the promotion of media literacy and user-empowerment instruments is not adopted as the only or primary solution to the regulation of OP liability, but rather as initiatives complementing other policy options.

8.2.3 Promoting self-regulation

Description. Under this option, EU institutions would further strengthen the use of self-regulatory instruments, such as the existing Code of Practice against Disinformation, where members of the industry adopt voluntary commitments and ensure industry-government coordination.

Benefits. This option would have the benefit of having relatively limited costs, and, provided that various stakeholders (such as EU institutions, NGOs, consumer associations, fundamental rights agencies etc.) are included in the dialogue, it would allow a certain degree of cooperation in identifying shared responsibilities and adequate solutions. Moreover, strengthening efforts towards self-regulation would enhance OPs' responsibility and accountability without hampering innovation, while up-to-date revisions of commitments and practices would ensure that OP regulation is in line with technological development. Indeed, private companies are in a privileged position to identify problems that deserve regulatory attention and devise effective solutions, and may perceive, understand and react to changes in their markets more quickly than governments, leading to faster and possibly more effective responses than those resulting solely from statutory regulation. Most importantly, pressure for the adoption of codes of conduct – together with user-empowerment tools (section 6.1, section 6.6) may prove particularly useful for finding common solutions on how to combat harmful yet not illegal content, which – not being clearly defined – is less suitable for notice-and-take-down actions.

Drawbacks. On the other hand, public sectors' objectives are not always aligned with companies' objectives, so relying on co- and self-regulation alone may lead to outcomes that do not perfectly match those of public regulators. Furthermore, extant initiatives have already been criticised for their sometimes reduced effectiveness, and it is unlikely that they would be capable of ensuring an optimal level of control and management of the digital environment unless complemented with hard law rules on OPs' duties and liability. In particular, limitations in the range of participants, vaguely formulated commitments, the frequent absence of clear objectives, and of measurable progress indicators, as well as the general lack of sanctions other than admonition and expulsion from the initiative, question whether OPs could truly autonomously manage the issue of illegal and harmful content, in both an effective and fully compliant – primarily with the fundamental rights of the users – manner. Indeed, while OPs could privilege clear cut solutions that could lead to excessive censorship and activism, the complexity of the matter and the relevance of the interests at stake, require more subtle and precise balancing (see, e.g., section 6.5).

Recommendations. For the aforementioned reasons, we suggest that the promotion of industry self-regulation is not adopted as the only or primary solution to the regulation of OPs' liability, but rather complements other policy options.

[310] See Acquisti (2010). The Economics of Personal Data and the Economics of Privacy. OECD 30 Years after the OECD Privacy Guidelines. OECD Conference Centre. 'If we take seriously the premise that consumers" privacy relies on knowledge and consent, the costs of getting consumers informed may be prohibitive. For the case of online privacy alone, McDonald and Cranor (2008) calculate that, if every US internet users perused the privacy policies of the sites she visits, the national opportunity cost for the time needed to read those policies would be on the order of $781 billion'.

8.2.4 Establishing co-regulation mechanism and tools

Description. Under this option, EU institutions and OPs would cooperate directly to reach optimal regulatory solutions under soft law and voluntary instruments. Such an effort could take place in a variety of modes:

- Building upon the traditional self-regulatory tools, with EU institutions – or specifically designated bodies – collaborating with members of the industry in both the development of the commitments and in monitoring their compliance. For example, said tools could take the form of 'audited self-regulation', where codes of conduct and practices would be subject to formal audit by a commonly agreed independent institution, such as the Online Platform Observatory, or a devoted European agency.[311]
- Creating and regulating national enforcement bodies (NEB) to oversee OP practices under the supervision of a central EU regulator, similar to the model employed under the GDPR through data protection authorities and the supervisory board. As suggested by other studies,[312] such NEB could be trusted with powers to launch investigations on OPs' failure to comply with legal obligations, sanction them, and compel data/algorithm transparency to ensure access to data.
- Creating of regulatory sandboxes, i.e. schemes that enable firms to test different solutions, e.g. algorithm-based content filters,[313] pursuant to plans agreed with and monitored by a dedicated competent authority.

Benefits. All the aforementioned solutions would allow stronger public oversight of OPs' practices, and the adoption of flexible and industry-driven regulatory schemes, capable of being constantly adjusted in the light of the assessments made through public oversight, as well as on the basis of the new technological developments or new challenges connected to the use of digital services. Overall, they could lead to a better understanding of risks, opportunities, recurrent obstacles and gaps, and allow firms, relevant stakeholders and supervisory authorities to communicate, exchange information and gain technical expertise, as well as reach suitable views on regulation.[314]

Drawbacks. The actual efficacy of this option would depend on the specific instrument adopted to implement it. For example, 'Building upon the traditional self-regulatory tools') (see section 8.2.3), being a voluntary measure, may still suffer from a lack of participation. Likewise, the costs would vary depending on the level of engagement of public bodies, the need to establish new agencies or authorities, and the level of resources attributed to them. Likewise, they would also vary depending on the type of support which the latter would grant to OPs (e.g. access to specialist expertise; access to digital innovation hubs).

Recommendations. For the aforementioned reasons, the adoption of co-regulatory solutions is highly recommended and preferred to the promotion of unsupervised self-regulatory tools. This, however, would in no way prevent policy-makers from adopting other solutions in combination with it. Indeed, particular synergies could be expected with the options in section 8.2.5 below.

---

[311] See Marsden and Meyer (2019). Regulating disinformation with artificial intelligence.

[312] Smith (2020). E-Commerce and the future Digital Services Act., p 77 and Committee on the Internal Market and Consumer Protection (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)).para 30 and 31

[313] Expert Group on Regulatory Obstacles to Financial Innovation (2019). 30 Recommendations on Regulation, Innovation and Finance., 71

[314] Ibid., 71-72

8.2.5 Adopting statutory legislation

Under this option, EU institutions would define OPs' duties and liabilities by means of binding regulation. Different models and approaches may be conceived, as analysed below.

8.2.5.1 Establishing clear and narrowly-tailored primary duties for OPs

Description. The EU institution could impose a series of duties on OPs on the management of their platforms' infrastructure and content-monitoring tools and techniques. Most importantly, these duties could be associated with the OPs' primary liability, that most commonly ought to be civil, at times administrative, and seldom – if ever – criminal, in nature.

As discussed in the recent policy debate, these obligations could include rules on the permitted use and functioning of algorithm-based filtering, on the removal of illegal content, notice-and-take-down rules, transparency, content-advertising services, and service interoperability (Chapter 5).[315] These rules could be developed according to a 'technology neutral' or a 'technology specific' approach, but – as clarified in section 8.1 above – we believe that only the latter could ensure that solutions are adequate for the problem that they are meant to address, and ensure the legal certainty required for a good regulatory environment. In other words, duties and corresponding liabilities should be conceived for specific domains, types of platforms, and policy concerns.

(i) Notice-and-take-down procedures, counter-notices and instruments for contesting removal. OPs could be obliged to adopt notice-and-take-down procedures, as well as counter-notices and instruments for contesting removal. In particular, NTD actions could be regulated through common principles and essential requirements defined at EU level,[316] while specific technical methods of implementation could be outlined in European harmonised standards – as currently happens with technical standards[317] – or in delegated acts, as in the regulation of drones,[318] which should be

[315] See, de Streel, Defreyne, Jacquemin, Ledger, Michel, Innesti, Goubet and Ustowski (2020). Online Platforms' Moderation of Illegal Content Online., Committee on Legal Affairs (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market. (2020/2018(INL))., Committee on the Internal Market and Consumer Protection (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)). European Commission (2020). IIA. Digital Services Act

[316] Husovec (2018). 'The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which is Superior? And Why?' Columbia Journal of Law & the Arts 42(1): 53-84.and Committee on the Internal Market and Consumer Protection (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL))., p. 9

[317] Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards, OJ C 136, 4.6.1985, 1–9; Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218, 13.8.2008, 30–47; Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, OJ L 218, 13.8.2008, 82–128; Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC, OJ L 218, 13.8.2008, 21–29.

For an overview of this approach, see https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en, and, more in detail, European Commission (2016). The 'Blue Guide' on the implementation of EU products rules 2016. For a description and an assessment of the product safety framework in the field of industrial robots, see Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3, Task 3&4.

[318] See Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance.), OJ L 152, 11.6.2019, 45–71, as amended by Commission Implementing Regulation (EU) 2020/639 of 12 May 2020 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations executed in or beyond the visual line of sight, OJ L 150, 13.5.2020, 1–31, Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, OJ L 152, 11.6.2019, 1–40.

specifically designed for particular types of infringement and specific types of OPs. All these mechanisms should respect procedural fairness for all the subjects involved.

(ii) Reporting obligations and procedural accountability. Furthermore, OPs could be subject to reporting obligations and harmonised rules of procedural accountability. Reporting obligations should be clear, specific and concise, and clearly expose the results of follow-up to removal decisions, to ensure that OPs do not engage in over-removal and impose excessive burdens on their users. Reports should be drafted and published in a comprehensive manner, to allow the post-evaluation and assessment of the correct compliance with the obligations resting upon them.[319] Moreover, large OPs' content management policies and mechanisms should be made subject to public review and advisory oversight,[320] to be carried out possibly by a newly created supervisory body, as suggested under section 8.2.4.

(iii) Specific duties for transaction-platforms. OPs that allow the trading and supply of goods and services on their infrastructures should be subject to an obligation to verify the identity of the traders based on a 'Know Your Business Customer' principle (e.g. by requesting information such as company registration number), to provide such information to users and third parties that have a legitimate interest, and to make sure that the information provided is accurate and up-to-date.[321] OPs should not allow the registration or creation of accounts for users that provide false, misleading or otherwise invalid information. When placing orders, OPs should inform the customers they are entering into a contract with the trader or the platform, as the case may be, and where the contract is concluded with a trader, the platform should provide the customer with the traders' identity and contact details.[322] Moreover, specific cooperation duties between OPs and market authorities could be strengthened, by requiring that 'once products have been identified as unsafe by the Union's rapid alert systems or by consumer protection authorities, it should be compulsory to remove products from the marketplace within 24 hours'.[323]

(iv) Algorithm-based filtering. A general obligation to adopt automated filtering and content recognition shall, at this stage, be excluded, as it would constitute an excessive burden for OPs, and, most importantly, it may lead to over-removal and infringements of users' freedoms and fundamental rights. If OPs choose to adopt automated filtering and content recognition tools, they should be mandated to comply with rules on algorithmic transparency, and ensure a 'right to an explanation' and request for human oversight, similar to that set in Article 22 GDPR.[324]

(v) Transparency on content managing. Given the opacity of filtering, ranking and preferential display algorithms, which can result among other things, in discrimination and the creation of echo chambers, OPs should specify clearly and unambiguously in their Terms of Use what type of content and activities is permitted, and what consequences may result from a breach.[325] Moreover, they should explain the 'exact parameters of their AI systems and how they can affect the choice or behaviour of their users, as

[319] See Heldt (2019). Reading between the lines and the numbers: an analysis of the first NetzDG reports.

[320] See Gillespie (2018). Platforms Are Not Intermediaries.

[321] Similarly see Dhar (2017). 'Should We Regulate Digital Platforms?' Big Data **5**(4): 277-278.

[322] See Busch, Dannemann, Schulte-Nölke, Wiewiórowska-Domagalska and Zoll (2016). Discussion Draft of a Directive on Online Intermediary Platforms., European Law Institute (2019). Model Rules on Online Platforms.

[323] Committee on the Internal Market and Consumer Protection (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)).

[324] See Marsden and Meyer (2019). Regulating disinformation with artificial intelligence.

[325] Committee on the Internal Market and Consumer Protection (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)).

well as the reasons and importance of such specific parameters as opposed to others'.[326] Likewise, an obligation of transparency could be imposed on OPs that provide review and reputational functions/systems. In this case, OPs should provide an explanation about how relevant information is collected, processed, and published as reviews. Essential requirements for the functionality of such reputational systems should be set by binding regulation (e.g. reviews must be published without undue delay, their date should be displayed, the most recent reviews should be displayed first by default, etc.) while the exact technical means for compliance should be left for the platform to decide.[327] Moreover, OPs that 'provide services consisting of offering programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, to inform, entertain or educate, using electronic communication networks, and the organisation of which is determined by the video-sharing platform provider, including by use of automatic means or algorithms, in particular by displaying, tagging and sequencing',[328] could be held responsible for administrating their platforms in full respect of a set of specific obligations. In this line, they could be obliged to maintain ideologically neutral services, create algorithms that foster and promote diversity of content, and offer options to users in selecting their settings for content, without the latter including the possibility to identify and disable fake accounts.[329]

(vi) Harmful content. While OPs may be called to promote the fight against harmful content, this solution should not result in OPs restricting freedom of speech and freedom of information. For this reason, regulatory-sandboxes are suggested above (section 8.2.4).

(vii) Innocent-third parties' injunctions. Moreover, it could be appropriate to positively harmonise a form of liability, in case OPs are ordered to cooperate in removing the infringement ('innocent third parties' injunctions'), and fail to comply, or do not do so in an adequate and timely manner.

Benefit. Clear obligations may provide greater certainty and safety for companies, users, and society, than the mere enactment of a general duty of care on OPs. This could be achieved by creating a list of such obligations to be updated over time.[330] Moreover, monetary awards ordered by enforcement authorities or courts against reprehensible platforms may be used to feed a no-fault scheme compensation fund, to be administrated by a centralised authority in Europe, as a possible solution to providing compensation under an RMA (section 8.1).

Drawbacks. The aforementioned instruments are expected to be costly and require major political coordination.

Recommendations. For the reasons stated above, the establishment of clear and narrowly-tailored primary duties for OPs is highly recommended. This, however, would in no way prevent policy-makers from adopting other solutions in combination. Indeed, particular synergies could be expected with the options in section 1)a)i)8.2.5.2 below.

[326] Ibid., p. 12.

[327] See European Law Institute (2019). Model Rules on Online Platforms.; Busch (2016). How to Regulate Online Rating and Review Systems in the Collaborative Economy.

[328] See Art. 1 (1) (b) (aa) of the AVSMD.

[329] Madiega (2020). Reform of the EU liability regime for online intermediaries.

[330] Committee on Legal Affairs (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market. (2020/2018(INL)).

8.2.5.2 Modifying OPs' secondary liability

Model A – Clarifying the conditions for liability exemptions under the ECD

Description. Under this option, the current baseline regime set out in the ECD would be maintained, and merely adjusted, to fill the gaps and uncertainties discussed in section 6.1, mostly adopting the interpretations and practices developed by the CJEU and European institutions' actual interpretations and practices. In particular, this option could serve to:

- Expressly ensure that the requirement of a 'service normally provided for remuneration' is met by entities who offer their services for free or under the 'freemium/premium model' and that it includes cases where digital content or digital services are not supplied against remuneration, but rather against user provided personal data, which works de facto as a counter-performance, in line with the solution adopted in the Digital Content and Service Directive;[331]
- Extend the notion of ISSP to cover new forms of OPs, such as cloud computing and storage, search engines,[332] online advertising platforms, collaborative platforms and social media,[333] allowing their activity to fall under the notion of 'hosting' as per Article 14 ECD,[334] possibly including services such as cloud computing and storage, collaborative platforms and social media.[335]
- Clarify whether activities such as ranking, indexing, provision of review systems, etc. are of a mere technical, automatic and passive nature (Recital 42 ECD) and thus covered by the exemption under Article 14 ECD.[336] Alternatively, it could be possible to overcome the distinction and apply the liability exemptions to all providers of digital intermediation services, both passive and active,[337] although certain experts advise against this option.[338]
- Expressly provide that the adoption of pro-active measures to fight illegal content online would not lead the OPs to qualify as 'active' platforms, with the result of losing the liability exemption under Article 14. Alternatively, an express 'Good Samaritan' rule could be adopted,[339] to ensure that all OPs – active or passive – are not dissuaded from monitoring the content hosted by their infrastructure.[340]
- Clarify what constitutes 'actual knowledge', or 'awareness', of 'illegal content or activity' – if a specific court order or notice is required, or if general awareness would suffice, and if

[331] See Directive (EU) 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. PE/26/2019/REV/1, OJ L 136, 22.5.2019, p. 1–27.

[332] See Husovec and De Steel (2020). The e-Commerce Directive as the cornerstone of the Internal Market. Study for the committee on Internal Market and Consumer Protection Luxembourg, Policy Department for Economic., p. 43

[333] See Lomba and Evas (2020). Digital Services Act. European added value assessment., Annex III, pp. 290-291. Also see Madiega (2020). Reform of the EU liability regime for online intermediaries., pp. 4 and 14.

[334] See van Hoboken, Quintais, Poort and van Eijk (2018). Hosting Intermediary Services and Illegal Content Online.

[335] See Sartor (2017). Providers Liability.

[336] See Madiega (2020). Reform of the EU liability regime for online intermediaries, p. 14. On whether advertising platforms can benefit from the ECD liability exemption in trade-mark infringement cases, please see Stalla-Bourdillon (2011). 'Uniformity v. Diversity of Internet Intermediaries' Liability Regime: Where does the ECJ stand?' Journal of International Commercial Law and Technology **6**(1): 51-61.

[337] See Sartor (2017). Providers Liability.

[338] Lomba and Evas (2020). Digital Services Act. European added value assessment., Annex III, p. 295.

[339] See Madiega (2020). Reform of the EU liability regime for online intermediaries, p. 17.

[340] Sartor (2017). Providers Liability. Contrary, see Lomba and Evas (2020). Digital Services Act. European added value assessment., Annex III, p. 295.

'constructive knowledge' could be included,[341] as well as what timeframe can be said to ensure an 'expeditious' reaction to the infringement;
- Clarify the distinction between 'specific content monitoring obligations' and 'general duty of care' to ensure that OPs are not urged to adopt over-detecting activities due to fear of liability.

Benefits. This solution would have relatively limited costs, leaving the essential elements of the status quo – harmonised negative conditions for secondary liability – unchanged; yet it would ensure further legal certainty by reforming the ECD in a way that clarifies its most debated concept/gaps, and would grant continuity with extant CJEU and national court interpretative practices.[342]

Drawbacks. No particular drawbacks are associated with this option. However, the level of legal certainty over the basic conditions of OPs' liability would remain highly fragmented, as they are left to Member State autonomy.

Recommendations. For the aforementioned reasons, clarifying the conditions for liability exemptions under the ECD is a highly recommended solution. This, however, would in no way prevent policy-makers from adopting other initiatives in combination. Indeed, particular synergies could be expected with the options in sections 8.2.2-8.2.4 above.

Model B – Establishing a harmonised regime of liability

Under this option, the EU institutions would radically change the current regulatory strategy and directly harmonise (at least some of the) conditions under which OPs may be held liable for the illegal content/conduct of their users. This may be achieved through two different strategies.

General harmonisation. According to this solution, OPs could be subject to a specific duty to act whenever they obtain credible evidence of illegal conduct that is to the detriment of other users, as well as take adequate measures to prevent harm. Failure to do so would make them liable for the damages deriving therefrom.[343] Whereas the ECD sets negative conditions for a harmonised liability exemption, this solution would set out some basic obligations and associate a secondary-liability thereto, covering the harm suffered by both the users of the platforms, as well as other persons that could be deemed as falling under the scope of protection of a platform-user-contract. This option can be considered as self-standing, or as complementing or replacing the liability exemption under Article 14 ECD. Moreover, it could constitute (an additional layer to) the baseline regime of liability, upon which other, sectoral systems of liability could insist.

Sectoral harmonisation. Indeed, one case where positive harmonisation of OPs' secondary liability may occur is that of damages suffered by users of transaction platforms because of the defective/harmful nature of the product or service offered by other users. Here, the level of control that the OPs exercise on the transaction and its users, is enough to justify a solution similar to that adopted by the US courts and discussed in section 6.8. In particular, it could be possible to envisage a form of strict and objective liability under the RMA described above, and which substantially reflects the current European regime for importers and distributors of defective products under Article 3 of the PLD.

[341] According to the CJEU in Case C-324/09 L'Oreal et al. v. eBay EU:C:2011:474, para. 120, the exemption of liability as under Article 14 of the E-Commerce Directive requires that an intermediary should not have been aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question.

[342] For a brief overview on how national and international courts analyse different OPs related provisions see Callamard (2017). 'Are courts re-inventing Internet regulation?' International Review of Law, Computers & Technology 31(3): 323–339.

[343] See Art. 10 of European Law Institute (2019). Model Rules on Online Platforms. and Sartor (2017). Providers Liability.

On the contrary, such OPs' strict secondary liability could prove to be less adequate in cases of damages caused by a breach of peer-to-peer contracts, unless the platform itself takes up certain responsibility, e.g. by setting specific warranties on the quality and security of the transaction, because the reduced capacity to adequately manage risk ex-ante or ex-post would create suboptimal incentives in policing users' activities. Instead, primary duties may be placed upon OPs to ensure that they: (i) identify and (ii) ascertain the reliability of their users – according to a 'Know-you-customer-approach'[344], as well as (iii) cooperate with the victim – ex post – in the identification of the alleged infringer.

Benefits Clear conditions for liability may provide greater certainty and safety for companies, users, and society alike, in such a more effective manner than what a general duty of care entails, also setting a level playing field for OPs across Europe. Moreover, the case-by-case provision of OPs' duties and corresponding liabilities under a RMA, could substantially improve users' protection, by further clarifying the applicable legal framework, thence ensuring maximum legal certainty.

Drawbacks. The aforementioned instruments are expected to increase Member States' and OPs' costs of compliance. The latter, in particular, may be problematic for Small-Medium Enterprises, limiting their capacity to penetrate the European digital services market. For these reasons, narrow-tailored specific forms of liability may be particularly important.

Recommendations. For the aforementioned reasons, the modification of OPs' secondary liability is highly recommended and, indeed, because of the greater legal certainty and uniformity associated with it, constitutes the preferred solution. This, however, would in no way prevent the policy-makers from adopting other options in combination with it. Indeed, particular synergies could be expected with the options in sections 8.2.2-8.2.5 and section 1)a)i)8.2.5.1 above.

[344] Committee on the Internal Market and Consumer Protection (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)).

9. Conclusions

Online platforms (OPs) have gained unprecedented economic and societal importance in the last decade, posing a series of regulatory concerns.

In particular, questions arise about their responsibility in ensuring a safe and secure online environment, where respect is granted to the users' fundamental rights and freedoms, and where the activities of both consumers and business users are adequately regulated. Indeed, OPs are subject to multiple rules on liability – summarised in Table 4 below – which results in a complex regulatory patchwork, comprising both (i) liabilities connected to the activities performed or the content uploaded by OP users and (ii) alternative sources of liability, such as OPs' contractual liability against both its business and consumer users, as well as those deriving from infringements of privacy and data protection law. With respect to the former, the regulatory framework is diverse and complex, consisting of the 'Safe Harbour' set in the ECD, and the sectoral rules provided in media law, IP law, product safety and product liability, protection of minors, hate speech, disinformation and voting manipulation, terrorist activities, etc.

This framework is comprised of both hard-law rules at EU and national level, as well as voluntary instruments such as codes of conduct and memoranda of understanding, which representatives of the industry signed, often with the facilitation or oversight of governmental institutions. Moreover, these rules have different – subjective and objective – scopes of application, with some applying transversally to potentially all OPs, and others applying only to specific types of OPs, infringements or activities.

Finally, in the call for an increase in OP's responsibility different approaches are found, ranging from the imposition of (i) specific duties that burden the platform despite the generalised liability exemption set out in the ECD,[345] (ii) obligations to inform and empower users and adopt procedural and technical tools, as well as (iii) duties to block, remove and prevent the re-upload of infringing material.

Overall, the system is incredibly complex and often underspecified, and it is difficult for the subjects involved to understand exactly when a given obligation applies to them, and what kind of behaviour is required.

This uncertainty may lead to two different, yet equally concerning alternative outcomes. The first being the risk of inducing OPs to limit their engagement in fighting online harmful/illegal content, by presenting themselves as 'mere intermediaries' to benefit from the liability exemption under the ECD. In such a perspective, they could limit their efforts to merely adjusting their terms of services and ensuring formal compliance with information duties, and other relevant obligations resting upon them. Alternatively, they might opt for an 'over-compliance' strategy, increasing the quantity, speed and automation of content-removal, without engaging in adequate contextualisation, or without giving space for counter-notices and rectification, resulting in an overall violation of users' fundamental rights and freedoms.[346]

For these reasons, establishing a clear set of obligations, narrow-tailored for specific types of platforms and infringement, appears to be fundamental. To this end, the classification criteria provided make it possible to depict a quite detailed matrix of possible specific issues and concerns.

[345] Similarly see Montagnani and Trapova (2019). Safe Harbors in Turmoil?

[346] In the same line, and based on an economic analysis of the uncertainties connected to the application of the ECD: Hornik and Villa Llera (2017), 'An Economic Analysis of Liability of Hosting Services: Uncertainty and Incentives Online', Bruges European Economic Research Papers 37/2017.

Within such an overall perspective, it is necessary to re-shape OPs' liability, taking into consideration the fact that the latter constitutes only **one element** of a broader normative framework, destined to interact with other regulatory instruments. In some cases, for example, non-liability-related tools and remedies are preferable to incentivise OPs to adopt an optimal level of content management and moderation. At the same time, OPs' civil liability may, instead, be directed towards purposes different from deterrence, such as prompt and full compensation of the harm suffered because of the infringement, regardless of any further consideration of fault or negligence.

Most importantly, the role attributed to liability rules, as well as their actual configuration, should not be drafted under a 'one-size-fits-all' or 'technology-neutral' approach, through the imposition of broad and under-specified duties of care.[347] On the contrary, regulation needs to be conceived as 'technology-specific', narrowly tailored on the type of risk/harm considered, as well as on various characteristics of the platforms involved.[348]

For this reason, the suggested approach relies on the interaction of different layers, and kinds of intervention.

Firstly, EU institutions should define OPs' duties and liabilities by means of binding rules, regulating the management of platforms' infrastructure and content-monitoring tools and techniques. Most importantly, these duties could be associated with the OPs' primary liability, which most commonly ought to be civil, at times administrative, and seldom – if ever – criminal, in nature.

Ideally, when flexibility and constant updates are required, these duties could be set through common principles and essential requirements defined at EU level,[349] and further specified in delegated acts or harmonised standards.

As for secondary liability, it would be appropriate to maintain a 'baseline' regulatory regime – to be supplemented and complemented by sector-specific rules, where the conditions for third-party liability could be directly harmonised. According to this solution, OPs could be subject to a specific duty to act whenever they obtain credible evidence of illegal conduct that is to the detriment of other users, as well as take adequate measures to prevent harm. Failure to do so would make them liable for the damages deriving therefrom. This option can be considered as self-standing, or as complementing or replacing the liability exemption under Article 14 ECD.

As for sectoral systems of liability, in addition to the specific regime already established for IP law, a system of strict and absolute liability could be established for large transaction platforms for the damage caused by the defective/harmful nature of the product or service offered by other uses. Here, the level of control that the OPs exercise over the transaction and their users is such as to justify a solution similar to that adopted by the US courts and discussed in section 6.8. In particular, it could be possible to envisage a form of strict and objective liability under the risk management approach (RMA) described above, and which substantially reflects the current European regime for importers and distributors of defective products under Article 3 of the PLD.

[347] Similarly see Committee on the Internal Market and Consumer Protection (2020). Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the Digital Services Act and fundamental rights issues posed (2020/2022(INI)).

[348] Similarly see Madiega (2020). Reform of the EU liability regime for online intermediaries., p. 9.

[349] Husovec (2018). Takedown or Staydown? Which is Superior? And Why?and Committee on the Internal Market and Consumer Protection (2020). Opinion on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL))., p. 9. Similarly see Ullrich (2017). 'Standards for duty of care? Debating intermediary liability from a sectoral perspective.' Journal of Intellectual Property, Information Technology and Electronic Commerce Law 8(2).

Table 4 - OPs' sources and rules on liability

Source of Liability	Legislative framework	Target	Measures	Soft law relevant initiatives	Self-regulation
Baseline (all types of illegal content)	Directive 2000/31/EC (E-Commerce Directive/ECD)	All (information society service providers)	Liability exemptions (mere conduit, chasing, hosting)	European Parliament resolution of 15 June 2017 on online platforms and the digital single market Communication from the Commission on Tackling Illegal Content online. COM(2017) 555 final Commission Recommendation on measures to effectively tackle illegal content online. C(2018) 1177 final	/
Media Law	Directive 2010/13/EU concerning the provision of audiovisual media services (Audio-visual Media Service Directive) amended by Directive (EU) 2018/1808	Video-sharing platform services	Procedural accountability	/	/
Online piracy, IP and copyrights infringement	Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market	Online content-sharing providers	Liability exemption if best efforts are employed	/	Memorandum of Understanding on online advertising and intellectual property rights Memorandum of understanding on the sale of counterfeit goods on the internet

Source of Liability	*Legislative framework*	*Target*	*Measures*	*Soft law relevant initiatives*	*Self-regulation*
	Directive 2004/48/EC on the enforcement of intellectual property rights Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society	Information society services providers	Injunctions/ preliminary measures	/	/
Child Protection	Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography	General (obligation set on Member States, no reference to OPs)	Blocking and removal measures	The European Strategy for a Better Internet for Children Safer Internet Centres and Alliance to better protect minors online	/
	Directive 2010/13/EU concerning the provision of audiovisual media services (Audio-visual Media Service Directive) amended by Directive (EU) 2018/1808	Video-sharing platform services	Procedural accountability	Global Alliance against Child Sexual Abuse and WeProtect Global Alliance	/
Illegal hate speech	Council Framework Decision 2008/913 on combatting certain forms of expressions of racism and xenophobia by means of criminal law	General (obligation set on Member States, no reference to OPs)	/	/	Code of Conduct on Countering Illegal Hate Speech Online (2016)
	Directive 2010/13/EU concerning the provision of audiovisual media services (Audio-visual Media Service Directive) amended by Directive (EU) 2018/1808	Video-sharing platform services	Procedural accountability	/	/

Source of Liability	Legislative framework	Target	Measures	Soft law relevant initiatives	Self-regulation
	The Network Enforcement Act (NetzDG) of 1 October 2017 Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet	Social networks Platform operators and search engines	Procedural accountability	/	/
Disinformation and voting manipulation	The Network Enforcement Act (NetzDG) of 1 October 2017 Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information	Social networks Platform operators	Procedural accountability	Commission Communication on Tackling online disinformation. COM/2018/236 final	Code of Practice on Disinformation (2018)
Terrorist content (provocation to commit a terrorist offence)	Directive (EU) 2017/541 on combating terrorism	General (obligation set on Member States, no reference to OPs)	Blocking and removal measures	Commission Recommendation on measures to effectively tackle illegal content online. C(2018) 1177 final	EU Internet Forum
	Directive 2010/13/EU concerning the provision of audiovisual media services (Audio-visual Media Service Directive) amended by Directive (EU) 2018/1808	Video-sharing platform services	Procedural accountability	Commission Proposal on a Regulation on preventing the dissemination of terrorist content online	/
Product Liability	Council Directive 85/374/EEC (Product Liability Directive)	Producers, importers, distributors, suppliers	Liability for defective and unsafe products	/	Product Safety Pledge
	Regulation (EU) 2019/1020 on market surveillance and compliance of products	Information society services providers	Notice and action	/	/
Contractual liability	P2C - general consumer law	Traders	Prohibited practices/blacklists	ELI Model Rules on Online Platforms	/

Source of Liability	*Legislative framework*	*Target*	*Measures*	*Soft law relevant initiatives*	*Self-regulation*
	P2B - Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services	Online intermediation services and online search engines	Transparency and procedural accountability	/	/
	C2C - general civil law provisions on contract formation, performance and remedies for breach	/	Contract formation Performance Remedies for breach	/	/
Data Protection	Regulation (EU) 2016/679 (General Data Protection Regulation/GDPR)	Controllers/processors	Rights and obligation for an effective personal data protection as a fundamental right Data protection by design and by default Security	/	/
	Directive 2002/58/EC (ePrivacy Directive)	Electronic communication services/digital mobile networks	Security in the processing of personal data Notification of personal data breaches Confidentiality of communication	Commission Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications	/

10. References

- (2011). The Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet.
- (2017). A Safer Internet for Minors. Statement of Purpose Alliance to Better Protect Minors Online.
- (2018). EU Code of Practice on Disinformation.
- (2018). "Memorandum of Understanding on online advertising and intellectual property rights."
- (2020). Product Safety Pledge. Voluntary commitment of online marketplaces with respect to the safety of non-food consumer products sold online by third party sellers.
- Access Now, ARTICLE 19, COMMUNIA association, Centrum Cyfrowe, Civil Liberties Union for Europe, Civil Rights Defenders, Creative Commons, dataskydd.net, Electronic Frontier Foundation, European Digital Rights (EDRi), Global Forum for Media Development, Homo Digitalis, Idec - Brazilian Institute of Consumer Defense, Open Knowledge Foundation, OSEPI, Panoptykon Foundation, Privacy International, Ranking Digital Rights, Rights International Spain and Xnet (2020). Joint statement in response to the inception impact assessments on a new competition tool ex ante regulatory instrument for large online platforms acting as gatekeepers Brussels.
- Acquisti, A. (2010). The Economics of Personal Data and the Economics of Privacy. OECD 30 Years after the OECD Privacy Guidelines. OECD Conference Centre.
- Armstrong, M. (2006). "Competition in two-sided markets." The RAND Journal of Economics 37(3): 668-691.
- Baistrocchi, P. (2003). "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce." Santa Clara High Technology Law Journal 19(1): 111-130.
- Batura, O., N. van Gorp and P. Larouche (2015). Online Platforms and the EU Digital Single Market. A response to the call for evidence by the House of Lord's internal market sub-committee Rotterdam.
- Bayer, J., P. Bard and E. Lorand (2020). Hate speech and hate crime in the EU and the evaluation of online content regulation approaches Lexembourg, P. D. f. C. R. a. C. Affairs.
- BEREC (2018). BEREC report on the impact of premium content on ECS markets and the effect of devices on the open use of the Internet.
- Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214–247.
- Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist 16(3): 291-314.
- Bertolini, A. (2020). Artificial Intelligence and Civil Liability Bruxelles, Policy Department for Citizens' Rights and Constitutional Affairs.
- Botta, M. and K. Wiedemann (2019). "To discriminate or not to discriminate? Personalised pricing in online markets as exploitative abuse of dominance." European Journal of Law and Economics: 1-24.
- Bradshaw, S. and P. Howard (2018). Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation Oxford.
- Brunner, L. (2016). "The Liability of an Online Intermediary for Third Party Content. The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia." Human Rights Law Review 16(1): 163–174.
- Busch, C. (2016). Crowdsourcing Consumer Confidence: How to Regulate Online Rating and Review Systems in the Collaborative Economy. European Contract Law and the Digital Single Market: Implications of the Digital Revolution. A. De Franceschi. Cambridge, Intersentia: 223-243.
- Busch, C., G. Dannemann, H. Schulte-Nölke, A. Wiewiórowska-Domagalska and F. Zoll (2016). "Research Group on the Law of Digital Services. Discussion Draft of a Directive on Online Intermediary Platforms." Journal of European Consumer and Market Law 5(4): 164-169.
- Busch, C., H. Schulte-Nölke, A. Wiewiórowska-Domagalska and Z. Fryderyk (2016). "The Rise of the Platform Economy: A New Challenge for EU Consumer Law?" Journal of European Consumer and Market Law 5(1): 3-10.

- Calabresi, G. and D. A. Melamed (1972). "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral." Harvard Law Review 85(6): 1089.
- Callamard, A. (2017). "Are courts re-inventing Internet regulation?" International Review of Law, Computers & Technology 31(3): 323–339.
- Coleman, J., S. Hershovitz and G. Mendlow (Winter 2015). Theories of the Common Law of Torts. The Stanford Encyclopedia of Philosophy. E. Zalta. https://plato.stanford.edu/archives/win2015/entries/tort-theories/.
- Committee on Legal Affairs (2020). Opinion of the Committee on Legal Affairs for the Committee on the Internal Market and Consumer Protection with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)).
- Committee on the Internal Market and Consumer Protection (2020). Draft Report with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)).
- Committee on the Internal Market and Consumer Protection (2020). Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the Digital Services Act and fundamental rights issues posed (2020/2022(INI)).
- Committee on Transport and Tourism (2020). Opinion of the Committee on Transport and Tourism for the Committee on the Internal Market and Consumer Protection with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)).
- De Steel, A. and P. Larouche (2016). An Integrated Regulatory Framework for Digital Networks and Services. A CERRE Policy Report Brussels, CERRE.
- de Streel, A., E. Defreyne, H. Jacquemin, M. Ledger, A. Michel, A. Innesti, M. Goubet and D. Ustowski (2020). Online Platforms' Moderation of Illegal Content Online. Law, Practices and Options for Reform Luxembourg, S. a. Q. o. L. P. Policy Department for Economic.
- Dhar, V. (2017). "Should We Regulate Digital Platforms?" Big Data 5(4): 277-278.
- Engels, S. and T. Fuhrmann (2018). "Network Enforcement Act in a nutshell." https://blogs.dlapiper.com/iptgermany/2018/01/31/network-enforcement-act-in-a-nutshell/ 2020.
- European Commission "Product safety rules. How product safety rules are defined and enforced in the EU." https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/product-safety-rules_en.
- European Commission (1996). Communication from the Commission. Illegal and harmful content on the Internet. COM(96) 487 Final Brussels, European Commission.
- European Commission (1996). Green Paper Liability for defective products. COM(1999)396 final Brussels, European Commission.
- European Commission (2012). Communication from the Commission. European Strategy for a Better Internet for Children. COM(2012) 196 final Brussels, European Commission.
- European Commission (2013). Report from the Commission on the functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet. COM(2013) 209 final Brussels, European Commission.
- European Commission (2014). Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law. COM(2014) 27 final Brussels, European Commission.
- European Commission (2016). Commission Staff Working Document Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices. SWD(2016) 163 final Brussels, European Commission.
- European Commission (2016). Commission Staff Working Document. Online Platforms Accompanying the document Communication on Online Platforms and the Digital Single Market. SWD(2016) 172 final Brussels, European Commission.

- European Commission (2016). Commission Staff Working Document. Preliminary Report on the E-commerce Sector Inquiry. SWD(2016) 312 final Brussels, European Commission.
- European Commission (2016). Communication from the Commission. A European agenda for the collaborative economy. COM(2016) 356 final Brussels, European Commission.
- European Commission (2016). Communication from the Commission. Online Platforms and the Digital Single Market Opportunities and Challenges for Europe. COM(2016) 288 final Brussels, European Commission.
- European Commission (2016). Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. COM(2016) 872 final Brussels, European Commission.
- European Commission (2017). Commission Staff Working Document on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for All. SWD(2017) 155 final Brussels, European Commission.
- European Commission (2017). Commission staff Working Document. Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights. SWD(2017) 431 final Brussels, European Commission.
- European Commission (2017). Communication from the Commission. Tackling Illegal Content Online. Towards an enchanced responsibility of online platforms. COM(2017) 555 final Brussels, European Commission.
- European Commission (2017). Final report on the E-commerce Sector Inquiry. COM(2017) 229 final Brussels, European Commission.
- European Commission (2017). Overview of the functioning of the Memorandum of Understanding on the sale of counterfeit goods via the internet. SWD(2017) 430 final Brussels, European Commission.
- European Commission (2017). Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM(2017) 10 final Brussels, European Commission.
- European Commission (2018). 1st Progress Report on the Implentation of the Product Safety Pledge.
- European Commission (2018). Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online. C(2018) 1177 final Brussels, European Commission.
- European Commission (2018). Commission Staff Working Document. Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. SWD(2018) 157 final Brussels, European Commission.
- European Commission (2018). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Tackling online disinformation: a European Approach. COM(2018) 236 final Brussels, European Commission.
- European Commission (2018). Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services. SWD(2018) 138 final Brussels, European Commission.
- European Commission (2018). Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation. JOIN(2018) 36 final Brussels, European Commission.
- European Commission (2018). Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online. COM(2018) 640 final Brussels, European Commission.
- European Commission (2019). 2nd Progress Report on the Implentation of the Product Safety Pledge.
- European Commission (2019). Joint Communication European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. Report on the implementation of the Action Plan Against Disinformation. JOIN(2019) 12 final Brussels, European Commission.

- European Commission (2020). Commission Staff Working Document. Report on the functioning of the Memorandum of Understanding on online advertising and intellectual property rights. SWD(2020) 167 final/2 Brussels, European Commission.
- European Commission (2020). Commission Staff Working Document. Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet. SWD(2020) 166 final/2 Brussels, European Commission.
- European Commission (2020). Communication from the Commission. Shaping Europe's digital future. COM(2020) 67 final Brussels, European Commission.
- European Commission (2020). Factsheet: Countering illegal hate speech online 5th evaluation of the Code of Conduct Brussels, D.-G. f. J. a. Consumers.
- European Commission (2020). Inception Impact Assessment. Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services. Ref. Ares(2020)2877686 Brussels.
- European Commission (2020). Inception Impact Assessment. Revision of Directive 2001/95/EC of the European Parliament and of the Council on general product safety. Ref. Ares(2020)3256809 Brussels, U. J. E. P. S. a. R. A. System.
- European Data Protection Board (2020). Guidelines 8/2020 on the targeting of social media users. Version 1.0.
- European Data Protection Supervisor (2018). Opinion 3/2018 on online manipulation and personal data.
- European Law Institute (2019). Report of the European Law Institute. Model Rules on Online Platforms Vienna.
- European Parliament (2017). European Parliament resolution of 15 June 2017 on online platforms and the digital single market (2016/2276(INI)).
- European Parliament (2019). European Parliament recommendation of 13 March 2019 concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties (2018/2115(INI)) Luxembourg.
- European Parliament (2019). European Parliament resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP)).
- European Parliament (2020). Digital Services Act: Improving the functioning of the Single Market European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)). TEXTS ADOPTED. Provisional edition.
- European Parliament (2020). Report with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)). Plenary sitting.
- European Union Agency for Fundamental Rights (2019). FRA Opinion – 2/2019 Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications Vienna.
- Evans, D. and R. Schmalensee (2008). Markets with Two-Sided Platforms. Issues in Competition Law and Policy (ABA Section of Antitrust Law). 1.
- Evans, D. and R. Schmalensee (2010). "Failure to Launch: Critical Mass in Platform Businesses." Review of Network Economics 9(4).
- Evans, D. and R. Schmalensee (2016). Matchmakers: The New Economics of Multisided Platforms. Boston, Massachusetts, Harvard Business Review Press.
- Expert Group on Regulatory Obstacles to Financial Innovation (2019). 30 Recommendations on Regulation, Innovation and Finance. Final Report to the European Commission Brussels.
- Filistrucchi, L., D. Geradin, E. Damme and P. Affeldt (2013). "Market Definition in Two-Sided Markets: Theory and Practice." Journal of Competition Law and Economics 10.

- Flash Eurobarometer 464 (2018). Report on fake news and disinformation online, C. T. Directorate-General for Communications Networks.
- Gawer, A. (2016). Online Platforms: Contrasting perceptions of European stakeholders A qualitative analysis of the European Commission's Public Consultation on the Regulatory Environment for Platforms.
- Gillespie, T. (2018). "Platforms Are Not Intermedieries." Georgetown Law Teechnology Review 2: 198.
- Goodman, E. and S. Livingstone (2018). "Protection of children online: does current regulation deliver?" https://blogs.lse.ac.uk/medialse/2018/11/27/protection-of-children-online-does-current-regulation-deliver/ 2020.
- Hacker, P. (2018). "UberPop, UberBlack, and the Regulation of Digital Platforms after the Asociacion Profesional Elite Taxi Judgment of the CJEU." European Review of Contract Law 14(1): 80-96.
- Hagiu, A. and J. Wright (2014). "Marketplace or Reseller?" Management Science 61(1).
- Hagiu, A. and J. Wright (2015). "Multi-Sided Platforms." International Journal of Industrial Organization 43: 162-174.
- Hausemer, P., J. Rzepecka, M. Dragulin, S. Vitiello, L. Rabuel, M. Nunu, A. Rodriguez Diaz, E. Psaila, S. Fiorentini, S. Gysen, T. Meeusen, S. Quaschning, A. Dunne, V. Grinevich, F. Huber and L. Baines (2017). Exploratory study of consumer issues in online peer-to-peer platform markets Brussels, D.-G. f. J. a. Consumers.
- Heerschap, N., N. Pouw and C. Atmé (2018). Measuring online platforms, CBS.
- Helbergera, N., T. Poellc and J. Piersonb (2018). "Governing online platforms: From contested to cooperative responsibility." The Information Society 34(1): 1-14.
- Heldt, A. (2019). "Reading between the lines and the numbers: an analysis of the first NetzDG reports." Internet Policy Review 8(2).
- High level Group (2018). A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation Belgium, C. a. T. Directorate-General for Communication Networks.
- Hornik, J. and C. Villa Llera (2017). "An Economic Analysis of Liability of Hosting Services: Uncertainty and Incentives Online." Bruges European Economic Research Papers 37/2017.
- Husovec, M. (2017). Injunctions against Intermediaries in the European Union: Accountable but Not Liable? Cambridge, Cambridge University Press.
- Husovec, M. (2018). "The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which is Superior? And Why?" Columbia Journal of Law & the Arts 42(1): 53-84.
- Husovec, M. and A. De Steel (2020). The e-commerce Directive as the cornerstone of the Internal Market. Study for the committee on Internal Market and Consumer Protection Luxembourg, S. a. Q. o. L. P. Policy Department for Economic.
- Iamiceli, P. (2019). "Online Platforms and the Digital Turn in EU Contract Law: Unfair Practices, Transparency and the (pierced) Veil of Digital Immunity." European review of contract law 15(4): 392–420.
- Kohl, U. (2013). "Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)." International Journal of Law and Information Technology 21(2): 187-234.
- Lambrecht, I., V. Verdoodt and J. Bellon (2018). "Platforms and commercial communications aimed at children: a playground under legislative reform?" International Review of Law, Computers & Technology 32(1): 58-79.
- Lazer, D. M. J., M. A. Baum, Y. Benkler, A. J. Berinsky, K. M. Greenhill, F. Menczer, M. J. Metzger, B. Nyhan, G. Pennycook, D. Rothschild, M. Schudson, S. A. Sloman, C. R. Sunstein, E. A. Thorson, D. J. Watts and J. L. Zittrain (2018). "The science of fake news. Addressing fake news requires a multidisciplinary effort." Social Science 359(6380): 1094-1096.
- Leistner, M. (2017). "Closing the book on the hyperlinks: brief outline of the CJEU's case law and proposal for European legislative reform." European Intellectual Property Review 39(6): 327-333.

- Livingstone, S., D. Tambini, N. Belakova and E. Goodman (2018). Protection of children online: does current regulation deliver? London.
- Lomba, N. and T. E. Evas (2020). Digital Services Act. European added value assessment Brussels, E. P. R. Service.
- Ludden, V., F. A. Hahn and A. Jeyarajah (2018). Evaluation of the implementation of the Alliance to better protect minors online, C. T. Directorate-General of Communications Networks.
- Madiega, T. (2020). Reform of the EU liability regime for online intermediaries. Background on the forthcoming digital services act Brussels, European Parliamentary Research Service.
- Marsden, C. and T. Meyer (2019). Regulating disinformation with artificial intelligence Brussels, E. P. R. Service.
- Marsden, C., T. Meyer and I. Brown (2020). "Platform values and democratic elections: How can the law regulate digital disinformation?" Computer Law & Security Review 36.
- Martens, B. (2016). An Economic Policy Perspective on Online Platforms. Institute for Prospective Technological Studies Digital Economy Working Paper 2016/05, J. R. C. I. f. P. T. Studies.
- Montagnani, M. L. and A. Trapova (2019). "New Obligations for Internet Intermediaries in the Digital Single Market - Safe Harbors in Turmoil?" Journal of Internet Law 22(7): 3-11.
- Nguyen, D. and M. Paczos (2020). Measuring the Economic Value of Data and Cross-Border Data Flows. A Business Perspective, OECD.
- Nooren, P., N. van Gorp, N. van Eijk and R. O. Fathaigh (2018). "Should We Regulate Digital Platforms? A New Framework for Evaluating Policy Options." Policy and Internet 10(3): 264-301.
- Nordemann, J. B. (2020). The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services Luxembourg, S. a. Q. o. L. P. Policy Department for Economic.
- Obergfell, E. I. and A. Thamer (2017). "(Non-)regulation of online platforms and internet intermediaries – the facts: Context and overview of the state of play." Journal of Intellectual Property Law & Practice 12(5): 435–441.
- OECD (2019). An Introduction to Online Platforms and Their Role in the Digital Transformation. Paris, OECD Publishing.
- Office for Harmonization in the Internal Market (2016). Digital Advertising on Suspected Infringing Websites.
- Palmerini, E., F. Azzarri, F. Battaglia, A. Bertolini, A. Carnevale, J. Carpaneto, F. Cavallo, A. Di Carlo, M. Cempini, M. Controzzi, B.-J. Koops, F. Lucivero, N. Mukerji, L. Nocco, A. Pirni, H. Shah, P. Salvini, M. Schellekens and K. Warwick (2014). Guidelines on Regulating Robotics.
- Palmerini, E. and A. Bertolini (2016). Liability and Risk Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice. R. Schulze and D. Staudenmayer. Baden-Baden, Nomos: 225-259.
- Palmerini, E., A. Bertolini, F. Battaglia, B.-J. Koops, A. Carnevale and P. Salvini (2016). "RoboLaw: Towards a European framework for robotics regulation." Robotics and Autonomous Systems 86: 78-85.
- Perset, K. (2010). The Economic and Social Role of Internet Intermediaries, OECD.
- Polinsky, M. A. and S. Shavell (2007). Handbook of Law and Economics, North-Holland.
- Polinsky, M. A. and S. Shavell (2009-2010). "The uneasy case for product liability." Harvard Law Review 123: 1437-1492.
- Research Group on the Law of Digital Services (2016). "Discussion Draft of a Directive on Online Intermediary Platforms." Journal of European Consumer and Market Law 5(4): 164-169.
- Riis, T. and S. F. Schwemer (2019). "Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation." Journal of Internet Law 22(7): 1–21.
- Riordan, J. (2020). A Theoretical Taxonomy of Intermediary Liability. Oxford Handbook of Online Intermediary Liability. G. Frosio. United States of America, Oxford University Press.

- Rochet, J.-C. and J. Tirole (2006). "Two-sided markets: a progress report." The RAND Journal of Economics 37(3): 645-667.
- Rosati, E. (2020). The Direct Liability of Intermediaries. Oxford Handbook of Online Intermediary Liability. G. Frosio. USA, Oxford University Press.
- Rosenfeld, M. (2002). "Hate speech in constitutional jurisprudence: a comparative analysis." Cardozo Law Review 24(4): 1523-1467.
- Sartor, G. (2017). Providers Liability: From the eCommerce Directive to the future. In-Depth Analysis for the IMCO Committee Brussels, P. D. o. E. a. S. Policy.
- Sartor, G. S. and A. Loreggia (2020). The impact of algorithms for online content filtering or moderation Brussels, Policy Department for Citizens' Rights and Constitutional Affairs.
- Savin, A. (2018). "Regulating Internet Platforms in the EU: The Emergence of the "Level playing Field"." Computer Law & Security Review 34(6): 1215-1231.
- Schulte-Nolke, H., I. Ruffer, C. Nobrega and A. Wieworowska-Domagalska (2020). 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 Luxembourg, S. a. Q. o. L. P. Policy Department for Economic.
- Secretary of State for Digital Culture Media & Sport and Secretary of State for the Home Department (2019). Online Harms White Paper UK.
- Senftleben, M. (2020). Oxford Handbook of Online Intermediary Liability. Intermediary Liability and Trade Mark Infringement: Proliferation of Filter Obligations in Civil Law Jurisdictions? G. Frosio. Oxford, Oxford University Press: 382-402.
- Shavell, S. (2007). Liability for Accidents. Handbook of Law and Economics. A. M. Polinsky and S. Shavell. Amsterdam, Elsevier: 142.
- Smith, M. (2020). Enforcement and cooperation between Member States. E-Commerce and the future Digital Services Act Luxembourg.
- Stalla-Bourdillon, S. (2011). "Uniformity v. Diversity of Internet Intermediaries' Liability Regime: Where does the ECJ stand?" Journal of International Commercial Law and Technology 6(1): 51-61.
- UK Government Office for Science (2020). Evidence and scenarios for global data systems. The Future of Citizen Data Systems United Kingdom.
- Ullrich, C. (2017). "Standards for duty of care? Debating intermediary liability from a sectoral perspective." Journal of Intellectual Property, Information Technology and Electronic Commerce Law 8(2).
- van Eijk, N., R. Fahy, H. van Til, P. Nooren, H. Stokking and H. Gelevert (2015). Digital platforms: an analytical framework for identifying and evaluating policy options The Hague.
- Van Gerven, W., J. Lever and P. Larouche (2000). Tort law. Oxford, Hart Publishing.
- Van Gorp, N. and O. Batura (2015). Challenges for Competition Policy in a Digitalised Economy. Study for the ECON Committee Brussels, P. D. A. E. a. S. Policy.
- van Hoboken, J., J. P. Quintais, J. Poort and N. van Eijk (2018). Hosting Intermediary Services and Illegal Content Online. An analysis of the scope of article 14 ECD in light of developments in the online service landscape Luxembourg, C. T. DG Communication Networks.
- von der Leyen, U. (2019). A Union that strives for more. My agenda for Europe by candidate for President of the European Commission. Political Guidelines for the Next European Commission 2019-2024.
- Walen, A. (Winter 2016 Edition). Retributive Justice. The Stanford Encyclopedia of Philosophy. E. Zalta. URL = <https://plato.stanford.edu/archives/win2016/entries/justice-retributive/>.
- White Bullet Solutions Limited (2020). Study on the impact of the Memorandum of Understanding on online advertising and intellectual property rights on the online advertising market Brussels, I. Directorate-General for Internal Market, Entrepreneurship and SMEs.
- Wiewiórowska-Domagalska, A. (2017). Online Platforms: How to Adapt Regulatory Framework to the Digital Age? Briefing PE 607.323.

Annex 1 - EU policy initiatives

From the Digital Market Strategy to the Communication on How to Tackle Illegal Content Online	
Commission's Communication on Online Platform and the Digital Single Market[350]	After having acknowledged the heterogeneous nature of OPs and identified their shared characteristics, the Commission stated that to correctly address the opportunities and challenges they bring about, the EU should adopt a balanced regulatory framework. In the Commission's view, such framework was meant to: (i) offer harmonised rules, to ensure uniformity, legal certainty and a level playing field; (ii) ensure compliance with existing EU rules on competition, consumer protection, personal data protection, fundamental rights and fundamental freedoms; (iii) ensure effective enforcement and cooperation between relevant authorities; (iv) combine hard law and soft-law instruments; and (v) follow a problem-driven approach, which could help identify the problems relating to specific OPs or content, evaluate the appropriateness of existing rules, and possibly revise them, without engaging in extensive and all-over-compassing regulation. In particular, the Commission advocated for interventions that would allow 'a level playing field for comparable digital services; responsible behaviour of OPs to protect core values; transparency and fairness for maintaining user trust and safeguarding innovation; open and non-discriminatory markets in a data-driven economy'. With regards to liability, the Commission claimed that – despite the ECD was designed at a time when OPs had different characteristic and roles than the ones they display today – public consultation had showed broad support for its main principles, and thus announced that, for the time being, its regime should remain valid. However, it identified a series of issues that were not adequately addressed, relating to the proliferation of online content that is harmful to minors, hate speech, allocation of revenues for the use of copyright-protected contents and enforcement of rules on counterfeit goods, incitement to terrorism, child sexual abuse and hate speech. In the Commission's view, these matters called for a regulatory update, through specific intervention, more effective notice-and-action tools, as well as by increasing the incentives for voluntary measures by service providers. As for fostering trust, transparency and fairness, the Commission stressed the need to inform and empower citizens and consumers, and to safeguard fair and innovation-friendly business environment, targeting B2B practices, and keep market open and non-discriminatory to foster a data driven economy.
Commission's Communication on a European agenda for the collaborative economy[351]	With this Communication, the Commission gave legal and policy making guidance for the Collaborative Economy sector, focusing of the following key issues: ➢ *Market access requirements*. For non-professional-service providers no such requirements exist, while standard EU rules on the provision of services regulate the activity of professional platforms' users (e.g. national market access requirements are allowed only if non-discriminatory, necessary for public-policy reasons and proportionate, in consideration of the collaborative business models' specific features). However, under existing law it is unclear when a service is provided 'professionally', suggesting that clear thresholds shall be established. With regards to platforms, as long as they provide 'a service normally provided for remuneration, at distance, by electronic means and at the individual request of a recipient of service', they are deemed as providing an information society service and cannot be subject to prior authorisation or similar requirements, pursuant to Artide 4 ECD. However, such conditions may be justified if they directly provide – rather than merely assisting platforms users in doing so – underlying services that are subject to authorisation and licensing (e.g. in the field of transportation or short-rent accommodation). Whether this is the case or not, shall be assessed on a case-by-case basis, with reference to the overall level of control exercised by the platform over the service (such as price, contractual terms, ownership of key assets). However, regulatory fragmentation shall as much as possible be avoided. ➢ *Liability*. The general liability regime for the provision of 'information society services' set by the ECD should be maintained, and possibly adjusted as to

[350] COM(2016) 288 final.

[351] COM(2016) 356 final.

From the Digital Market Strategy to the Communication on How to Tackle Illegal Content Online	
	incentivise pro-active measures to tackle illegal content online, which providers are reluctant to adopt as they fear losing the exemptions under the ECD. However, the aforementioned regime does not exclude that platforms may be held liable because of their own activities (e.g. when non-compliant with privacy and data protection rules), and – conversely – infringement of their primary legal duties has not direct impact on the intermediary liability-regime set out in the ECD. ➢ *Protection of users.* EU consumer law applies to any collaborative platform that qualifies as trader engaging in commercial practices with a consumer, and the same goes for the B2C relationships established directly between platform's users, while it does not apply to peer-to-peer relations. Thus, clear and common criteria are required to assess whether users qualify as consumers or business, whereas the actual assessment can only be done on a case-by-case basis. Drawing from national experience and from the Commission Guidance on the UCPD[352], Member States shall seek a balanced approach to ensure a high level of consumer protection, while not imposing disproportionate burdens on individuals who provide services without qualifying as traders; such assessment shall be based, *inter alia*, on the frequency of the services, the profit-seeking motive and the level of turnover. Trust-building mechanisms shall be used as much as possible for the purpose of ensuring consumer protection, also as an alternative to legislative interventions.
European Parliament Resolution on OPs and the digital single market[353]	Acknowledging both the difficulty and limited policy-relevance of a 'one-size-fits-all' definition of OPs, and the need to ensure legal certainty among all stakeholders involved, the European Parliament suggested 'that OPs should be distinguished and defined in their relevant sector-specific legislation at EU level according to their characteristic, classification and principles and following a problem-driven approach', calling on the Commission to address the barriers in the single market that are hindering their growth, especially with regards to SME. It also stressed the need to create a level playing field, both between online and offline services, and among different services offered by different platforms, advocating for tailor made solutions that could account for each type of platforms' specificity to ensure fair competition and equal footings (e.g. size), avoid monopolies or abuse of dominant position, also by fighting dangerous lock-in situation for users. It also called for a harmonisation of the rights of rectification, counterstatement and forbearance, and the creation of a level playing field with regards to claims for damages against platforms arising from the circulation of disparaging facts that create persistent harm for users. Taking account of the results of the public consultation – showing relative support for the current framework contained in the ECD, but also highlighting the need to eliminate certain flaws in its enforcement – the European Parliament argued for a clarification of the liability regime as to allow platforms to comply with their responsibilities and the rules on liability, enhance legal certainty and increase user confidence, and for measures that could re-balance the unfair distribution of value deriving from the distribution of creative content due to the uncertain status of online services under copyright and e-commerce law. On this matter, it suggested that platforms on which a significant volume of protected work are stored and made available to the public (unless 'passive', and thus covered by the exemption in Article 14 ECD) should conclude license agreements with relevant right holders, to ensure fair profit-sharing with authors, creators and relevant right holders, and underlines that such license agreements and their implementation must respect users' exercise of their fundamental rights. Moreover, the European Parliament urged 'OPs to strengthen measures to tackle illegal and harmful content' in an efficient manner, for instance 'by applying due diligence while maintaining a balanced and innovation friendly approach'. It solicited the Commission to clarify the notice and takedown procedures, as well as provide guidance on voluntary measures aimed at addressing such content. It stressed the need for OPs to combat illegal goods and unfair practices through regulatory

[352] SWD(2016) 163 final.

[353] European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI)).

From the Digital Market Strategy to the Communication on How to Tackle Illegal Content Online	
	measures complemented by effective self-regulatory measures (e.g. through clear terms of use and appropriate mechanisms to identify offenders, or by setting up specialised moderation teams and tracing dangerous products) or hybrid measures, as well as the need to comply with data protection rules. The European Parliament also stressed the need to inform and empower citizens and consumers, especially clarifying the issue of data access, data ownership and liability, and called on the Commission to evaluate the current regulatory framework on this regard. It then asked for technical solutions ensuring compliance with the relevant legislation (e.g. privacy by design and by default), and cooperation among authorities. It urged platform to adopt clear comprehensive and fair terms and conditions, high standards of consumer protection also in C2C, stressing the importance of providing users with clear impartial and transparent information on the criteria used to filter, rank, sponsor, personalise and or review information presented to them, calling on the Commission to address issues connected to the functioning of platforms' review systems. On a related note, the European Parliament expressed its concern about lack of transparency and fairness in B2B relations – e.g. search results, data use and pricing, unilateral changes in terms and conditions, promotion of adverting or sponsored results, unfair terms and condition, abuse of the dual role of platforms as intermediaries and competitors – and called for a targeted legislative intervention on the matter.
Commission's Communication on tackling illegal content and enhancing responsibility of OPs [354]	The Commission' Communication laid down a series of principles addressed to OPs, national authorities, Member States and other relevant stakeholders, which became core pillars in the policy debate on illegal content online, namely: ➢ *Detecting and notifying illegal content*. OPs should systematically enhance their cooperation with competent authorities in Member States, which, in turn, should ensure that courts are able to effectively react against illegal content online, and enable stronger (cross-border) cooperation between authorities. Effective points of contact should be established, and, where appropriate, effective digital interfaces should be set up to facilitate their interaction, as well as to allow general cooperation within the content governance cycle. As far as notice procedures are concerned, the Commission stressed the importance of trusted flaggers, calling on platform to grant them fast-track notice-procedures and cooperation tools, providing for mutual information exchange, and evaluated the possibility of agreeing EU-wide criteria for their identification. OPs should establish easy, accessible and user-friendly notification mechanism, and designed them in such a way as ensure their high-quality, i.e. having sufficient precision and substantiation, as to allow swift and informed follow ups. Finally, the Commission highlights the importance of incentivising proactive measures – including automatic tools and tools meant to avoid re-upload of removed content –, by OPs for detecting illegal content, and suggests that they should not, in themselves, lead to a loss of the liability exemption under the ECD, by qualifying the online platform as 'active'. ➢ *Removing illegal content*. OPs must take down illegal content expeditiously once they are made or become aware of its existence to avail themselves of the exemption set out in Article 14 ECD. Removal times and procedures for different forms of illegal content should be clearly reported in transparency reports. Promptness is of paramount importance where serious harm is at stake (e.g. incitement to terrorism), and the Commission commits to considering the possibility of setting fixed timeframes. Evidence of criminal offences obtained in the context removal should be transmitted to law enforcement authorities, in compliance with the law (e.g. Regulation (EU) 2016/679). OPs should provide a clear, easily understandable and sufficiently detailed explanation in their terms of service, regarding both the type of content permitted/non permitted (either because illegal, or because it is merely not allowed by the platforms themselves), and the procedures for contesting contest removal decisions. OPs should publish sufficiently detailed transparency reports (number and type of notices received and actions taken, time taken for processing, source of the notification, counter

[354] COM(2017) 555 final.

From the Digital Market Strategy to the Communication on How to Tackle Illegal Content Online	
	notices and relative response), to be published at least once per year. Finally, regarding the safeguards to be taken against over-removal and abuse of the system, online platform should offer simple online counter-notice procedures and ensure reasoned follow ups, and they should use of out-of-court dispute settlement bodies to resolve disputes about counter-notices whenever possible. ➢ *Preventing the re-appearance of illegal content*. OPs should take measures to refrain users from repeatedly uploading illegal content of the same nature, and use and develop automatic tools are encouraged, provided that they are transparently described in the platforms' terms of services, accompanied by a reversibility safeguard. Access to relevant databases (such as the Database of Hashes) should be available to all OPs, in respect of the appropriate data protection legislation.
Commission's Recommendation on Measures to Effectively tackle illegal content online[355]	The Commission's Recommendation proposed a series of measures to be adopted by Member States and OPs to ensure quick and proactive detection, removal and prevention of reappearance of illegal content, to be defined according to the 'what is illegal offline is illegal online' principle. Those measures consist in: ➢ *Clearer 'NTD action' procedures*. OPs were asked to provide easy and transparent rules for notifying illegal content and fast-track procedures for 'trusted flaggers'. At the same time, they were asked to inform content providers and give them the opportunity to contest the action, eventually avoiding the removal of licit content. ➢ *More efficient tools and proactive technologies*. OPs were asked to provide clear notification systems, as well as proactive tools for the detection and removal of illegal content, in particular in cases of terrorism and child sexual abuse, counterfeited goods and – in general – of content which is potentially highly harmful and does not require contextualisation to qualify as illegal. The Recommendation identified a series of measures to effectively reduce the uploading and sharing of terrorist propaganda online, including the obligations for companies not to host terrorist content and to remove such content within one hour of its flagging by law enforcement authorities and Europol. ➢ *Stronger safeguards to ensure fundamental rights*. OPs were requested to put in place effective and appropriate safeguards, including human oversight and verification where automated tools and filters are used, to ensure that decisions to remove content are accurate, well-founded and fully respectful of fundamental rights, (freedom of expression, privacy and data protection in particular). ➢ *Closer cooperation with authorities*. OPs were asked to promptly inform law enforcement authorities upon evidence of a serious criminal offence, or reasons to suspect threat to life of safety of users or third parties, deriving from the illegal content present carried over their infrastructure or service. ➢ *Special attention to small companies*. Finally, the recommendation advocated for the adoption of voluntary arrangements, tools for sharing experiences and best practices, as well as technological solutions, including those enabling automatic detection, with the aim of benefitting smaller platforms, which may lack the necessary resources and experiences to adopt a higher degree of governance for tackling content online. However, and most importantly, the adoption of all these measures was expressly stated as not affecting the liability regime set out in ECD (Article 12-15 ECD).

[355] C(2018) 1177 final.

Annex 2 - Legal definitions of online platforms

Instrument	*Scope of application*	*Definitions and references to online platforms*
Directive 2000/31/EC (E-Commerce Directive)[356]	Article 1 ➢ The Directive approximates certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-curt dispute settlements, court actions and cooperation between Member States. ➢ The Directive complements Community law applicable to information society services without prejudice to the level of protection for, public health and consumer interests. ➢ The Directive does no have innovative effects on private international law or the jurisdictions of Courts. ➢ The Directive does not apply to the following fields: taxation, application of the Directives 95/46/EC and 97/66/EC (information society services), cartel law, activities of notaries or equivalent professions involving the exercise of public authority, representation of a client and defence of his interests before the courts, gambling activities.	Article 2 ➢ *Information Society Services*: any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (as per Article 1(2) of Directive 98/34/EC, amended by Directive 98/48/EC).[357] ➢ *Service Provider*: 'any natural or legal person providing an information society service'. ➢ *Established Service Provider* is 'a service provider who pursue an economic activity using a fixed establishment for an indefinite period. Such establishment does not consist of the presence and use of the technical means and technologies required to provide the service'. ➢ *Recipient of the Service* is 'any natural or legal person who uses an information society service, for the purposes of seeking information or making it accessible'.
Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services[358]	Article 1 ➢ The Directive provides a high level of consumer protection so as to contribute to the efficiency of the internal single market, through rules on: conformity of digital content/ digital service with the contract; remedies, and modalities for their exercise, in case of lack of such conformity/ failure to supply; modification of digital content/ service. Article 3 The Directive applies to: ➢ Contracts where the trader supplies/ undertakes to supply	Article 2 ➢ *Digital Service* means: (a) a service that allows the consumer to create, process, store or access data in digital form; (b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service. ➢ *Digital Environment* means hardware, software and any network connection used by the consumer to access or make use of digital content or a digital service.

[356] See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

[357] See Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 204, 21.7.1998, p. 37–48.

[358] See Directive (EU) 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 (Text with EEA relevance.), PE/26/2019/REV/1, OJ L 136, 22.5.2019, p. 1–27.

Instrument	Scope of application	Definitions and references to online platforms
	digital content/ digital services to the consumer and the consumer: (a) pays or undertakes to pay a price; (b) provides or undertakes to provide personal data to the trader (not if the personal data provided is uniquely processed to supply the digital content/ digital service by the trader or to allow the trader to comply with legal requirements he is subjected to, and the trader does not process those data for any other purpose). ➢ Digital content/ digital services developed in accordance with the consumer's specifications. ➢ Any tangible medium which serves exclusively as a carrier of digital content (considering the limitations in Article 5 and 13). The Directive does not apply to: ➢ digital content/ digital services which are incorporated in or inter-connected with goods within the meaning of Article 2(3) and which are provided with the goods under a sales contract concerning those goods, irrespective of whether such digital content or digital service is supplied by the seller or by a third party. In the event of doubt as to whether the supply of incorporated or inter-connected digital content or an incorporated or inter-connected digital service forms part of the sales contract, the digital content or digital service shall be presumed to be covered by the sales contract. ➢ contracts regarding: (a) the provision of services other than digital services; (b) electronic communications services, as defined in Article 2(4) of Directive (EU) 2018/1972, except number-independent interpersonal communications services as defined in Article 2(7) of the same Directive; (c) healthcare as defined in Article 3(a) of Directive 2011/24/EU; (d) gambling services, including lotteries, casino games, poker games and betting transactions, by electronic means or any other technology for facilitating communication and at the individual request of a recipient of such services; (e) financial services as defined in Article 2(b) of Directive 2002/65/EC; (f) software offered by the trader under a free	➢ Recital (18)*: '[…] *Platform providers* could be considered to be traders under this Directive if they act for purposes relating to their own business and as the direct contractual partner of the consumer for the supply of digital content or a digital service. Member States should remain free to extend the application of this Directive to platform providers that do not fulfil the requirements for being considered a trader under this Directive'. *[notion explicitly mentioned but not defined]

Instrument	Scope of application	Definitions and references to online platforms
	and open-source licence, where the consumer does not pay a price and the personal data provided by the consumer are exclusively processed by the trader for the purpose of improving the security, compatibility or interoperability of that specific software; (g) the supply of digital content made available to the general public other than by signal transmission as a part of a performance or event, such as digital cinematographic projections; (h) digital content provided in accordance with Directive 2003/98/EC of the European Parliament and of the Council by public sector bodies of the Member States. ➢ to the elements of the contract concerning the digital content/digital service, when a single contract between the same trader and the same consumer includes in a bundle element of supply of digital content/ digital service and elements of the provision of other services or goods ➢ Article 19 does not apply where a bundle, within the meaning of Directive (EU) 2018/1972, includes elements of an internet access service as defined in Article 2(2) of Regulation (EU) 2015/2120 or a number-based interpersonal communications service as defined in Article 2(6) of Directive (EU) 2018/1972. Without prejudice to Article 107(2) of Directive (EU) 2018/1972, the effects that the termination of one element of a bundle contract may have on the other elements of the bundle contract shall be governed by national law.	
Directive (EU) 2019/2161 as regards the better enforcement and modernisation of Union consumer protection rules [359]	Article 4 (2) b) Amends Article 3 of Directive 2011/83/EU which shall also apply where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the	Art.3 Amendment to Article 2 (n) of Directive 2005/29/EC: ➢ *Online Marketplace* means a 'service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers'.

[359] See Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance), PE/83/2019/REV/1, OJ L 328, 18.12.2019, p. 7–28.

Instrument	Scope of application	Definitions and references to online platforms
	digital content which is not supplied on a tangible medium or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.	➢ *Provider of an online marketplace* is any trader which provides an online marketplace to consumer.
Directive 2011/83/EU on consumers rights [360]	Article 3 ➢ It applies to any contract concluded between a trader and a consumer. It shall also apply to contracts for the supply of water, gas, electricity or district heating, including by public providers, to the extent that these commodities are provided on a contractual basis ➢ It does not apply to contracts: (a) for social services, including social housing, childcare and support of families and persons permanently or temporarily in need, including long-term care; (b) for healthcare as defined in point (a) of Article 3 of Directive 2011/24/EU, whether or not they are provided via healthcare facilities; (c) for gambling, which involves wagering a stake with pecuniary value in games of chance, including lotteries, casino games and betting transactions; (d) for financial services; (e) for the creation, acquisition or transfer of immovable property or of rights in immovable property; (f) for the construction of new buildings, the substantial conversion of existing buildings and for rental of accommodation for residential purposes; (g) which fall within the scope of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours; (h) which fall within the scope of Directive 2008/122/EC of the European Parliament and of the Council of 14 January 2009 on the protection of consumers in respect of certain aspects of timeshare, long-term holiday product, resale and exchange contracts; (i) which, in accordance with the laws of Member States, are established by a public office-holder who has a	Recital (20) ➢ '[…] The notion of an organised distance sales or service-provision scheme should include those schemes offered by a third party other than the trader but used by the trader, such as an *online platform*. It should not, however, cover cases where websites merely offer information on the trader, his goods and/or services and his contact details'. Recital (24) ➢ '[…] The use of *online platforms* for auction purposes which are at the disposal of consumers and traders should not be considered as a public auction within the meaning of this Directive'.

[360] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, Text with EEA relevance, OJ L 304, 22.11.2011, p. 64–88

Instrument	Scope of application	Definitions and references to online platforms
	statutory obligation to be independent and impartial and who must ensure, by providing comprehensive legal information, that the consumer only concludes the contract on the basis of careful legal consideration and with knowledge of its legal scope; (j) for the supply of foodstuffs, beverages or other goods intended for current consumption in the household, and which are physically supplied by a trader on frequent and regular rounds to the consumer's home, residence or workplace; (k) for passenger transport services, with the exception of Article 8(2) and Articles 19 and 22; (l) concluded by means of automatic vending machines or automated commercial premises; (m) concluded with telecommunications operators through public payphones for their use or concluded for the use of one single connection by telephone, Internet or fax established by a consumer.	
Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods [361]	Article 3 It applies to: ➢ Sales contracts between consumers and sellers; ➢ Digital content or digital services which are incorporated in or inter-connected with goods [Article 2(5)(b)] and are provided with the goods under the sales contract, irrespective of whether such digital content or digital service is supplied by the seller or by a third party. In the event of doubt the digital content or digital service shall be presumed to be covered by the sales contract. It does not apply to: ➢ any tangible medium which serves exclusively as a carrier for digital content; ➢ any goods sold by way of execution or otherwise by authority of law; ➢ Member States may exclude the sale of second-hand goods sold at public auction, and of living animals.	Article 2(5)(b) ➢ *Goods* are any tangible movable items that incorporate/are inter-connected with digital content/digital service in such a way that the absence of it would prevent the goods from performing their functions ('*goods with digital elements*'). Article 2 (6) ➢ *Digital Contents* are data which are produced and supplied in digital form. Article 2 (7) ➢ *Digital Service* is a service that (a) allows the consumer to create, process, store or access data in digital form; or (b) allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service; Recital 23: ➢ *Platform providers** could be considered to be sellers under this Directive if they act for purposes relating to their own

[361] See Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.), PE/27/2019/REV/1, OJ L 136, 22.5.2019, p. 28–50

Instrument	Scope of application	Definitions and references to online platforms
		business and as the direct contractual partner of the consumer for the sale of goods. Member States should remain free to extend the application of this Directive to platform providers that do not fulfil the requirements for being considered a seller under this Directive. *[notion explicitly mentioned but not defined]
Directive 2002/58/EC (ePrivacy Directive)[362]	Article 1 ➢ It harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community. ➢ The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for the protection of the legitimate interests of subscribers who are legal persons. ➢ This Directive does not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law. Article 3 This Directive applies to: ➢ The processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community. ➢ Subscriber lines connected to digital exchanges and to subscriber	Article 2(g) ➢ *Value Added Service* is any service which requires the processing of traffic data/location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof. The Directive addresses directly electronic communication services/digital mobile networks and without defining them. Some references can be found in: Recital (5) ➢ '[…] The development of the information society is characterised by the introduction of new *electronic communications services*. Access to *digital mobile networks* has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk'. Recital (33): ➢ 'Therefore, in order to preserve the privacy of the user, Member States should encourage the development of *electronic communication service* options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card'. Recital (35)

[362] See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47

Instrument	Scope of application	Definitions and references to online platforms
	lines connected to analogue exchanges (but only the provisions of Article 8, Article 10 and Article 11). Recital 10: ➢ In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.	➢ '[…] However, in addition, *digital mobile networks* may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers […] Article 5 ➢ 'Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available *electronic communications services*, through national legislation […]'. Article 9(1) ➢ 'Where location data other than traffic data, relating to users or subscribers of *public communications networks* or publicly available *electronic communications services*, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service […]'. Definitions provided under Directive 95/46/EC and Directive 2002/21/EC shall apply.
Regulation (EU) 2016/679 (General Data Protection Regulation/GDPR)[363]	Article 2 This Regulation applies to: ➢ The processing of personal data wholly or partly by automated means/ the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system; This Regulation does not apply to the processing of personal data: ➢ in the course of an activity which falls outside the scope of Union law; ➢ by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;	The GDPR addresses electronic communication services/digital mobile networks and without defining them. Some references can be found in: Recital 49: ➢ The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and

[363] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

Instrument	Scope of application	Definitions and references to online platforms
	➢ by a natural person in the course of a purely personal or household activity; ➢ by competent authorities for the purposes of the prevention, investigation, detection/prosecution of criminal offences/the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. ➢ the by the Union institutions, bodies, offices and agencies, in which case Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98. The Regulation does not prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by *providers of electronic communications networks and services* and by *providers of security technologies and services*, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to *electronic communications networks* and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.
Regulation (EU) 2019/1020 on market surveillance and compliance of products [364]	Article 2 This Regulation applies to: ➢ Products that are subject to the 'Union harmonisation legislation (Annex I), in so far as there are no specific provisions with the same objective in it. ➢ Article 25-28 to products covered by Union law in so far as there are no specific provisions relating to the organisation of controls on products entering the Union market in Union law. This Regulation does not: ➢ prevent market surveillance authorities from taking more specific measures as in Directive 2001/95/EC. ➢ prejudice the application of Art.12 - 15 of Directive 2000/31/EC.	Article 3 ➢ (15) *Online Interface* is any software, including a website, part of a website or an application, that is operated by/on behalf of an economic operator, and which serves to give end users access to the economic operator's products; ➢ (13) *Economic Operator* is the manufacturer, the authorised representative, the importer, the distributor, the fulfilment service provider or any other natural or legal person who is subject to obligations in relation to the manufacture of products, making them available on the market or putting them into service in accordance with the relevant Union harmonisation legislation. ➢ (*14) Information Society Service Provider* is a provider of a service as defined in Article 1(1)(b) of Directive (EU) 2015/1535 [See Directive (EU) 2015/1535 below]

[364] See Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance.), PE/45/2019/REV/1, OJ L 169, 25.6.2019, p. 1–44.

Instrument	Scope of application	Definitions and references to online platforms
		There are many references to a generic '*Digital Environment*', without any further explicit clarification: Recital (34) ➢ '[…] Those powers should be sufficiently robust to tackle the enforcement challenges of Union harmonisation legislation, along with the challenges of *e-commerce and the digital environment* and to prevent economic operators from exploiting gaps in the enforcement system by relocating to Member States whose market surveillance authorities are not equipped to tackle unlawful practices. […]'. Recital (37) ➢ '[…] Market surveillance authorities should be able to request economic operators, including those in the *digital value chain*, to provide all the evidence, data and information necessary'. Recital (41) ➢ 'In the *digital environment* in particular, market surveillance authorities should be able to bring non-compliance to an end quickly and effectively, notably where the economic operator selling the product conceals its identity or relocates within the Union or to a third country in order to avoid enforcement […]'.
Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [365]		Article 1(1)(b) ➢ *Service* is any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. ➢ For the purposes of this definition: (i) 'at a distance' means without the parties being simultaneously present; (ii) 'by electronic means' means service sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

[365] See Directive (EU) 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 (Text with EEA relevance), OJ L 241, 17.9.2015, p. 1–15

Instrument	Scope of application	Definitions and references to online platforms
		(iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.
Commission Notice on the market surveillance of products sold online (2017/C 250/01)[366]		Section 3.3.2. Online intermediary services providers ➢ Economic operators can sell products directly to consumers or other end-users through web shops and can also use marketplaces provided by *online platforms*. ➢ […]Hosting is a service where an intermediary service provider, such as an online market place or an *online platform*, merely passively stores on its server — and makes it available to the public — information provided by the recipient of the service, such as an online seller of products.[…] ➢ Certain economic operators carry out various types of activities: *hosting services, trade under their own names, provide other services linked to e-commerce*. The competent authorities always have to determine in the given case in which quality the economic operator or website is to be considered. Section 5.2 Corrective actions specific to products sold online ➢ Where products are offered for sale online, national law can in some cases permit market surveillance authorities to request specific corrective actions from *online intermediary service providers (for example providers of hosting services, such as online platforms)* to remove or disable access to information concerning non-compliant and unsafe products from their website.
Regulation (EU) 2019/1148 on the marketing and use of explosives precursors[367]	Governs the marketing and use of explosives precursors. Article 2 It applies to:	Article 3 ➢ (10) *Economic Operator* is any natural or legal person/public entity or group of such

[366] See Commission Notice on the market surveillance of products sold online (Text with EEA relevance.), C/2017/5200, OJ C 250, 1.8.2017, p. 1–19

[367] See Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013, OJ L 186, 11.7.2019, p. 1–20

Instrument	Scope of application	Definitions and references to online platforms
	➢ The substances listed in Annexes I and II and to mixtures and substances that contain those substances It does not apply to: ➢ (a) articles as defined in point (3) of Article 3 of Regulation (EC) 1907/2006' ➢ (b) pyrotechnic articles as defined in point (1) of Article 3 of Directive 2013/29/EU of the European Parliament and of the Council; ➢ (c) pyrotechnic articles intended for non-commercial use in accordance with national law by the armed forces, law enforcement authorities or fire services; (d) pyrotechnic equipment falling within the scope of Directive 2014/90/EU of the European Parliament and of the Council (9); ➢ (e) pyrotechnic articles intended for use in the aerospace industry; ➢ (f) percussion caps intended for toys; ➢ (g) medicinal products that have been legitimately made available to a member of the general public on the basis of a medical prescription in accordance with the applicable national law.	persons/entities which make regulated explosives precursors available on the market, either offline or online, including on online marketplaces ➢ (11) *Online Marketplace* is a provider of an intermediary service that allows economic operators and members of the general public (professional users or other economic operators), to conclude transactions regarding regulated explosives precursors via online sales or service contracts, either on the online marketplace's website or on an economic operator's website that uses computing services provided by the online marketplace Recital (14) ➢ *Online marketplaces act as mere intermediaries* between economic and members of the general public, professional users or other economic operators. Therefore, online *marketplaces should not fall under the definition of an economic operator* and should not be required to instruct their personnel involved in the sale of restricted explosives precursors regarding the obligations under this Regulation or to verify the identity and, where appropriate, the licence of the prospective customer, or to request other information from the prospective customer. However, given the central role which online marketplaces play in online transactions, including as regards the sales of regulated explosives precursors, they should inform their users who aim to make regulated explosives precursors available through the use of their services of the obligations under this Regulation in a clear and effective manner. In addition, online marketplaces should take measures to help ensure that their users comply with their own obligations regarding verification, for instance by offering tools to facilitate the verification of licences. Given the increasing significance of

Instrument	Scope of application	Definitions and references to online platforms
		online marketplaces for all kinds of supply and the importance of this procurement channel, including for terrorist purposes, online marketplaces should be subject to the same detection and reporting obligations as economic operators, although procedures to detect suspicious transactions should be properly adapted to the specific online environment.
Commission Communication on Tackling Illegal Content Online. COM(2017) 555 final[368]	The aim is: ➢ to step up the fight against illegal content online in cooperation with national authorities, Member States and other relevant stakeholders; ➢ to facilitate and intensify the implementation of good practices for preventing, detecting, removing and disabling access to illegal content so as to ensure the effective removal of illegal content, increased transparency and the protection of fundamental rights online.	➢ The following references are made: '*Online platforms* also provide the main access point to information and other content for most people on the internet today, be it through *search engines, social networks, micro-blogging sites, or video-sharing platforms*. […] These platforms connect billions of users with vast quantities of content and information1 and provide innovative services to citizens and business'. ➢ *'Those online platforms which mediate access to content* for most internet users carry a significant societal responsibility in terms of protecting users and society at large and preventing criminals and other persons involved in infringing activities online from exploiting their services. The *open digital spaces they provide* must not become breeding grounds for, for instance, terror, illegal hate speech, child abuse or trafficking of human beings, or spaces that escape the rule of law'. 'Most *online platforms* offer hosting services of content uploaded by their users'. ➢ 'A *hosting service* is an *information society service* consisting of the storage of information provided by a recipient of the service. This category can cover a variety of actors, from *online marketplaces, video-sharing platforms, social networks, blogging websites or review websites, to users' comments' sections in news pages'*.

[368] See COM(2017) 555 final.

Instrument	*Scope of application*	*Definitions and references to online platforms*
Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final)[369]	Follows-up on the above-mentioned Communication, reflecting the level of ambition set out therein and giving effect thereto, while taking due account of and building on the important progress made through those voluntary arrangements.	Recital (1) ➢ 'Internet and *service providers active on the Internet* contribute significantly to innovation, economic growth and job creation in the Union. Many of those service providers play an essential role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and reception of information, opinions and ideas'. Recital (15) ➢ '*Providers of hosting services* play a particularly important role in tackling illegal content online, as they store information provided by and at the request of their users and give other users access thereto, often on a large scale. This Recommendation therefore primarily relates to the activities and responsibilities of those providers. However, where appropriate, the recommendations made can also be applied, *mutatis mutandis*, in relation to other *online services providers*'.
Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society[370]	Article 1 It applies to: ➢ Legal protection of copyright and related rights in the framework of the internal market, with particular emphasis on the information society. Except for Article 11, this Directive does not affect existing Community provisions relating to: ➢ the legal protection of computer programs; ➢ rental right, lending right and certain rights related to copyright in the field of intellectual property; ➢ copyright and related rights applicable to broadcasting of programmes by satellite and cable retransmission; ➢ the term of protection of copyright and certain related rights; ➢ the legal protection of databases.	Recital (59) ➢ 'In the *digital environment*, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities'. (Generic references, without definition/description)
Directive (EU) 2019/790 on copyright and related	Article 1 ➢ Aims to harmonise further Union law applicable to copyright and related rights in the framework of	Article 2 ➢ (5) *Information Society Service* is a service within the meaning of point (b) of Article 1(1) of

[369] See C(2018) 1177 final.

[370] See 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, OJ L 167, 22.6.2001, p. 10–19

Instrument	Scope of application	Definitions and references to online platforms
rights in the Digital Single Market[371]	the internal market, in particular, digital and cross-border uses of protected content. ➢ Lays down rules on exceptions and limitations to copyright and related rights, on the facilitation of licences, as well as rules which aim to ensure a well-functioning marketplace for the exploitation of works and other subject matter. ➢ With the exception of Article 24, it does not affect Directives 96/9/EC, 2000/31/EC, 2001/29/EC, 2006/115/EC, 2009/24/EC, 2012/28/EU and 2014/26/EU.	Directive (EU) 2015/1535 defined above) ➢ (6) *Online Content-sharing Service Provider* is a provider of an information society service of which the main/one of the main purposes is to store and give the public access to a large amount of copyright-protected works/other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes. The Directive does not apply to: ➢ Providers of services, such as not-for-profit online encyclopaedias, not-for-profit educational and scientific repositories, ➢ open source software-developing and-sharing platforms, ➢ providers of electronic communications services as defined in Directive (EU) 2018/1972, ➢ online marketplaces, ➢ business-to-business cloud services and cloud services that allow users to upload content for their own use Recital (61) ➢ '[…] Online content-sharing services providing access to a large amount of copyright-protected content uploaded by their users have become a main source of access to content online. *Online services* are a means of providing wider access to cultural and creative works and offer great opportunities for cultural and creative industries to develop new business models. […]'. Recital (62) ➢ 'The definition of an *online content- sharing service provider* laid down in this Directive should target only online services that play an important role on the online content market by competing with other online content services, such as online audio and video streaming services, for the same audiences'.

[371] See Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.), PE/51/2019/REV/1, OJ L 130, 17.5.2019, p. 92–125.

Instrument	Scope of application	Definitions and references to online platforms
Directive (EU) 2018/1972establishing the European Electronic Communications Code[372]	Article 1 Its aims are to: ➢ implement an internal market in electronic communications networks and services that results in the deployment and take-up of very high capacity networks, sustainable competition, interoperability of electronic communications services, accessibility, security of networks and services and end-user benefits; ➢ ensure the provision throughout the Union of good quality, affordable, publicly available services through effective competition and choice, to deal with circumstances in which the needs of end-users, including those with disabilities in order to access the services on an equal basis with others, are not satisfactorily met by the market and to lay down the necessary end-user rights. It does not affect the regime of: ➢ obligations imposed by national law in accordance with Union law or by Union law in respect of services provided using electronic communications networks and services; ➢ measures taken at Union or national level, in accordance with Union law, to pursue general interest objectives, in particular relating to the protection of personal data and privacy, content regulation and audio-visual policy; ➢ actions taken by Member States for public order and public security purposes and for defence; ➢ Regulations (EU) No 531/2012 and (EU) 2015/2120 and Directive 2014/53/EU. ➢ compliance of their processing of personal data with Union data protection rules.	Article 2 ➢ *Electronic communications network* is a transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed; ➢ *Very high capacity network* is either an electronic communications network which consists wholly of optical fibre elements at least up to the distribution point at the serving location, or an electronic communications network which is capable of delivering, under usual peak-time conditions, similar network performance in terms of available downlink and uplink bandwidth, resilience, error-related parameters, and latency and its variation; network performance can be considered similar regardless of whether the end-user experience varies due to the inherently different characteristics of the medium by which the network ultimately connects with the network termination point; ➢ *Electronic communications service* is a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content

[372] See Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance., PE/52/2018/REV/1, OJ L 321, 17.12.2018, p. 36–214

Instrument	Scope of application	Definitions and references to online platforms
		transmitted using electronic communications networks and services, the following types of services: (a) 'internet access service' as defined in Article 2(2)(2) of Regulation (EU) 2015/2120; (a) interpersonal communications service; (b) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting; ➢ *Interpersonal communications service* is 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; ➢ *Number-based interpersonal communications service* is an interpersonal communications service which connects with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which enables communication with a number or numbers in national or international numbering plans; ➢ *Number-independent interpersonal communications service* is an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans; ➢ *Public electronic communications network* is an electronic communications network used

Instrument	Scope of application	Definitions and references to online platforms
		wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points; ➢ *Associated service* is a service associated with an electronic communications network or an electronic communications service which enables or supports the provision, self-provision or automated-provision of services via that network or service, or has the potential to do so, and includes number translation or systems offering equivalent functionality, conditional access systems and electronic programme guides (EPGs), as well as other services such as identity, location and presence service; ➢ *End user* a user not providing public electronic communications networks or publicly available electronic communications services; ➢ *Provision of an electronic communications network* is the establishment, operation, control or making available of such a network; ➢ *Application programming interface ('API')* is the software interface between applications, made available by broadcasters or service providers, and the resources in the enhanced digital television equipment for digital television and radio services; ➢ *Small-area wireless access point* is low-power wireless network access equipment of a small size operating within a small range, using licenced radio spectrum or licence-exempt radio spectrum or a combination thereof, which may be used as part of a public electronic communications network, which may be equipped with one or more low visual impact antennae, and which allows wireless access by users to electronic communications networks regardless of the underlying network topology, be it mobile or fixed; ➢ *Radio local area network ('RLAN')* is low-power wireless access

Instrument	Scope of application	Definitions and references to online platforms
		system, operating within a small range, with a low risk of interference with other such systems deployed in close proximity by other users, using, on a non-exclusive basis, harmonised radio spectrum; ➢ *Operator* is an undertaking providing or authorised to provide a public electronic communications network or an associated facility; ➢ *Voice communications service* is a publicly available electronic communications service for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international numbering plan; ➢ *Total conversation service* is a multimedia real time conversation service that provides bidirectional symmetric real time transfer of motion video, real time text and voice between users in two or more locations;
Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet[373]	The purpose of this Memorandum of Understanding is to establish a code of practice in the fight against the sale of counterfeit goods over the internet and to enhance collaboration between the signatories including and in addition to Notice and Take-Down procedures. The MoU will also set an example for other stakeholders that are not signatories to this MoU.	➢ *'Internet Platform' is* any information society service provider whose service is used by third parties to initiate online the trading of physical goods, and which is operated by a signatory of the MoU, to he extent so indicated by the service provider.
Directive 2011/62/EU (the Falsified Medicine Directive)[374]		Recital 25: ➢ The public should be assisted in identifying *websites which are legally offering medicinal products for sale at a distance to the public*. A common logo should be established, which is recognisable throughout the Union, while allowing for the identification of the Member State where the person offering medicinal products for sale at a distance is established. The Commission should develop the design for such a logo. Websites

[373] See (2011). The Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet.

[374] See Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products Text with EEA relevance, OJ L 174, 1.7.2011, p. 74–87

Instrument	Scope of application	Definitions and references to online platforms
		offering medicinal products for sale at a distance to the public should be linked to the website of the competent authority concerned. The websites of the competent authorities of Member States, as well as that of the European Medicines Agency ('the Agency'), should give an explanation of the use of the logo. All those websites should be linked in order to provide comprehensive information to the public. Article 85c ➢ Without prejudice to national legislation prohibiting the offer for sale at a distance of prescription medicinal products to the public by means of information society services, Member Statesshall ensure that *medicinal products are offered for sale at a distance to the public by means of information society services* as defined in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (*) under the following conditions: [] the address of the *website used for that purpose* and all relevant information necessary to identify that website is notified to the Member State.
Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services[375]	Article 1 It applies to: ➢ *Online intermediation services and online search engines* provided/ offered to be provided, to business users and corporate website users, that have their place of establishment or residence in the Union and that, through those online intermediation services or online search engines, offer goods/services to consumers located in the Union, irrespective of the place of establishment/residence of the	Article 2 ➢ *Online Intermediation Services are services* which: (a) constitute information society services ex Article 1(1)(b) of Directive (EU) 2015/1535; (b) allow business users to offer goods/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) are provided to business users on the basis of

[375] See Regulation (EU) 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 (Text with EEA relevance), PE/56/2019/REV/1, *OJ L 186, 11.7.2019, p. 57–79.*

Instrument	Scope of application	Definitions and references to online platforms
	providers of those services and irrespective of the law otherwise applicable. It does not: ➢ apply to online payment services/to online advertising tools/online advertising exchanges, which are not provided with the aim of the facilitating the initiation of direct transactions and which do not involve a contractual relationship with consumers. ➢ affect national civil law, in particular contract law, such as the rules on the validity, formation, effects or termination of a contract, in so far as the national civil law rules are in conformity with Union law, and to the extent that the relevant aspects are not covered by this Regulation. ➢ prejudice Union law applicable in the areas of judicial cooperation in civil matters, competition, data protection, trade secrets protection, consumer protection, electronic commerce and financial services. Recital (2) ➢ This Regulation addresses such potential frictions in the online platform economy.	contractual relationships between the provider of those services and business users which offer goods or services to consumers; ➢ *Provider of Online Intermediation Services* is any natural or legal person which provides/offers to provide online intermediation services to business users ➢ *Online Search Engine* is a digital service that allows users to input queries in order to perform searches of all websites/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; ➢ *Provider of online search engine* is any natural or legal person which provides, or which offers to provide, online search engines to consumers; ➢ *Corporate website user* is any natural or legal person which uses an Online Interface, meaning any software, including a website or a part thereof and applications, including mobile applications, to offer goods or services to consumers for purposes relating to its trade, business, craft or profession; Recital (1) ➢ *Online intermediation services* are key enablers of entrepreneurship and new business models, trade and innovation, which can also improve consumer welfare and which are increasingly used by both the private and public sectors. They offer access to new markets and commercial opportunities allowing undertakings to exploit the benefits of the internal market. They allow consumers in the Union to exploit those benefits, in particular by increasing their choice of goods and services, as well as by contributing to offering competitive pricing online, but they also raise challenges that need to be addressed in order to ensure legal certainty. Recital (2)

Instrument	Scope of application	Definitions and references to online platforms
		➢ *Online intermediation services* can be crucial for the commercial success of undertakings who use such services to reach consumers.
Regulation (EU) 2017/1128 on cross-border portability of online content services in the internal market[376]	Article 1 ➢ To guarantee that subscribers to portable online content services (lawfully provided in their Member State of residence) can access and use them when temporarily present in a Member State other than their Member State of residence, so as to create a common approach in the Union to the cross-border portability of online content services.	Article 2 ➢ *Online Content Service* is a service (as defined in Articles 56-57 TFEU) that a provider lawfully provides to subscribers in their Member State of residence on agreed terms and online, which is portable and which is: (i) an audio-visual media service as defined in Article 1(a) of Directive 2010/13/EU; (ii) a service mainly useful to access to/use of, works, other protected subject-matter or transmissions of broadcasting organisations, whether in a linear or an on-demand manner ➢ *Portable* is a feature of an online content service whereby subscribers can effectively access and use the online content service in their Member State of residence without being limited to a specific location.
Commission Communication on a European Strategy for a Better Internet for Children. COM/2012/0196 final[377]	Aims to: ➢ Stimulate the production of creative and educational online *content* for children as well as promoting positive online experiences for young children; ➢ Scale up awareness and empowerment including teaching of digital literacy and online safety in all EU schools; ➢ Create a safe environment for children through age-appropriate privacy settings, wider use of parental controls and age rating and content classification; ➢ Combat child sexual abuse material online and child sexual exploitation.	Paragraph 2. ➢ 'A series of policies have been developed over the years at the European level to support children. However, they were often specific, e.g. focusing on media channels or *technological platforms* and have not been combined in a coherent framework […]'. Paragraph 2.1.2. ➢ 'The Commission will support *interoperable platforms* for tools ensuring access to age-appropriate content (such as white lists/child-friendly browsers) while considering the issue of continuous quality control'. […]'Industry should: engage in private-public partnerships to support the development of interactive tools and *platforms providing educational and awareness materials* for teachers and children, building on existing initiatives'. Footnote (27)

[376] See Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ L 168, 30.6.2017, p. 1–11

[377] See COM(2012) 196 final.

Instrument	Scope of application	Definitions and references to online platforms
		➢ […] The 'Safer Social Networking Principles for the EU', signed by *social networking service providers*, commits them to raising awareness of safety education messages, ensuring age-appropriate services, empowering users through tools and technology, providing easy-to-use reporting mechanisms, responding to notifications of illegal content or conduct, enabling and encouraging a safe approach to personal information and privacy, and assessing means for reviewing illegal or prohibited content/conduct […]. No definition for platforms is provided.
Directive 2010/13/EU concerning the provision of audiovisual media services (Audio-visual Media Service Directive)[378]	It aims to create and ensure the proper functioning of a single European Union market for audiovisual media services, while contributing to the promotion of cultural diversity and providing an adequate level of consumer and child protection.	Article 1 (1) ➢ (a) *Audio-visual media service* is: a service as defined by Articles 56-57 of the TFUE, where the principal purpose of the service or a dissociable section thereof is devoted to providing programmes, under the editorial responsibility of a media service provider, to the general public, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of Article 2(a) of Directive 2002/21/EC; such an audio-visual media service is either a television broadcast as defined in point (e) of this paragraph or an on-demand audio-visual media service as defined in point (g) of this paragraph; audio-visual commercial communication;' ➢ (aa) *Video-sharing platform service* is a service as defined by Articles 56-57 of the TFEU, where the principal purpose of the service/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

[378] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance), OJ L 95, 15.4.2010, p. 1–24

Instrument	Scope of application	Definitions and references to online platforms
		educate, by means of electronic communications networks within the meaning of Article 2(a) of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing." ➢ (da) *Video-sharing Platform Provider* is the natural or legal person who provides a video-sharing platform service ➢ (d) *Media service provider*' is the natural or legal person who has editorial responsibility for the choice of the audio-visual content of the audio-visual media service and determines the manner in which it is organised.
Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[379]	It sets forth: ➢ Minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children, child pornography and solicitation of children for sexual purposes. ➢ Provisions to strengthen the prevention of those crimes and the protection of the victims thereof.	Recital 12: ➢ Serious forms of sexual abuse and sexual exploitation of children should be subject to effective, proportionate and dissuasive penalties. This includes, in particular, various forms of sexual abuse and sexual exploitation of children which are facilitated by the use of information and *communication technology*, such as the online solicitation of children for sexual purposes via *social networking websites and chat rooms*.
Commission Communication on tackling online disinformation: a European Approach. COM(2018) 236 final[380]	Aims to: ➢ first, to improve transparency regarding the origin of information and the way it is produced, sponsored, disseminated and targeted in order to enable citizens to assess the content they access online and to reveal possible attempts to manipulate opinion. ➢ second, to promote diversity of information, in order to enable citizens to make informed decisions based on critical thinking, through support to high quality journalism, media literacy, and the rebalancing of the relation between	Paragraph 1 ➢ 'The *online platforms* that distribute content, particularly *social media, video-sharing services and search engines*, play a key role in the spread and amplification of online disinformation. Paragraph 3.1.1 ➢ 'There are growing expectations that *online platforms* should not only comply with legal obligations under EU and national law, but also act with appropriate responsibility in views of their central role so as to ensure a safe online

[379] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, p. 1–14

[380] COM(2018) 236 final.

Instrument	Scope of application	Definitions and references to online platforms
	information creators and distributors. ➢ third, to foster credibility of information by providing an indication of its trustworthiness, notably with the help of trusted flaggers, and by improving traceability of information and authentication of influential information providers. ➢ fourth, to fashion inclusive solutions. Effective long-term solutions require awareness-raising, more media literacy, broad stakeholder involvement and the cooperation of public authorities, online platforms, advertisers, trusted flaggers, journalists and media groups.	environment, to protect users from disinformation, and to offer users exposure to different political views'. ➢ The Commission will convene a multi-stakeholder forum on disinformation, to provide a framework for an efficient cooperation among relevant stakeholders, including *online platforms*, the advertising industry and major advertisers, media and civil society representatives, and to secure a commitment to coordinate and scale up efforts to tackle disinformation. Paragraph 3.3 ➢ 'A majority of respondents to the public consultation considered that educating and empowering users to better access and use online information and informing users when content is generated or spread by a bot are measures *online platforms* can take that would have a strong impact on preventing the spread of disinformation'. Paragraph 2.2 ➢ '*Social networking technologies* are manipulated to spread disinformation through a series of sequential steps: (i) creation; (ii) amplification through social and other online media; and (iii) dissemination by users'. Paragraph 3.5 ➢ 'The network will use the data gathered by the *secure online platform* on disinformation referred to in Section 3.1.2 in order to design outreach activities aimed at countering false narratives about Europe and tackling disinformation, within and outside the EU'. Paragraph 3.1.1 ➢ 'Ensure that *online services* include, by design, safeguards against disinformation; this should, for example, include detailed information on the behaviour of algorithms that prioritise the display of content as well as development of testing methodologies'. Many synonyms for an affine concept, but no definition.

Instrument	*Scope of application*	*Definitions and references to online platforms*
Joint Communication. Action Plan against Disinformation. JOIN(2018) 36 final[381]	➢ It focuses on how to deal with disinformation both within the EU and in its neighborhood. Efforts to strengthen the Strategic Communication Task Forces of the European External Action Service will play a key role here. ➢ Other actions aim to strengthen coordinated and joint responses to disinformation, to mobilise the private sector to make sure that it delivers on its commitments in this field, and to improve the resilience of society to the challenges that disinformation creates.	Pillar 2 ➢ The initial signatories are: Facebook, Google, Twitter and Mozilla as well as the trade association representing *online platforms*, (EDIMA) and trade associations representing the advertising industry and advertisers (EACA, IAB Europe, WFA and UBA). Pillar 2.1.3 ➢ The Commission will continue working with the Cooperation Network and *Platform Providers* on fostering the development and the voluntary use of systems for the secure identification of suppliers of information based on the highest security and privacy standards, including the possible use of verified pseudonyms. Pillar 3 ➢ *Online Platforms*, advertisers and the advertising industry have a crucial role to play in tackling the disinformation problem, as its scale is directly related to the platforms' ability to amplify, target and spread disinformation messages of malicious actors. ➢ *Large online platforms* should immediately: ensure security of placement and transparency of political advertising, based on effective due diligence checks of the identity of the sponsors; close down fake accounts active on their services; identify automated bots and label them accordingly. ➢ *Online platforms* should alco cooperate with the national audio-visual regulators and with independent fact-checkers and researchers to detect and flag disinformation campaigns in particular during election periods and to make fact-checked content more visible and whispered. [Just some, among other possible examples, to underline that the concept of Platform/Platform provider is considered relevant/fundamental but still not defined]
EU Code of Practice on Disinformation[382]	➢ Representatives of online platforms, leading social networks,	Par II.B

[381] See JOIN(2018) 36 final.

[382] See (2018). Code of Practice on Disinformation.

Instrument	Scope of application	Definitions and references to online platforms
	advertisers and advertising industry agreed on a self-regulatory Code of Practice to address the spread of online disinformation and fake news. ➢ It applies within the framework of existing laws of the EU and its Member States and must not be construed in any way as replacing or interpreting the existing legal framework. ➢ Does not prejudice other initiatives aiming at tackling Disinformation on platforms.	➢ Avoiding the misplacement of advertising on *online disinformation sites* requires further refinement of already widely used brand safety tools to successfully continue to meet this challenge, in recognition of the nature of this content.
Directive (EU) 2017/541 on combating terrorism[383]	➢ It establishes minimum rules concerning the definition of criminal offences and sanctions in the area of terrorist offences, offences related to a terrorist group and offences related to terrorist activities, as well as measures of protection of/support and assistance to victims of terrorism. ➢ It applies to offences perpetrated both online and offline, but it refers only to the generic concept of Internet or online contents without any further specification or clarification regarding their very meaning.	Recital (22) ➢ […] Whichever basis for action or method is chosen, Member States should ensure that it provides an adequate level of legal certainty and predictability for users and *service providers* and the possibility of judicial redress in accordance with national law. Recital (23) ➢ […] No general obligation should be imposed on *service providers* to monitor the information which they transmit or store, nor to actively seek out facts or circumstances indicating illegal activity. Furthermore, *hosting service providers* should not be held liable as long as they do not have actual knowledge of illegal activity or information and are not aware of the facts or circumstances from which the illegal activity or information is apparent […].
Report of the European Law Institute Model Rules on Online Platforms[384]	The scope is to provide a set of rules that contribute to fairness and transparency in the relations between platform operators and platform users. ➢ Represents a possible model for national, European and international legislators as well as a source of inspiration for self-regulation and standardisation. ➢ It is to be used in relation to platforms which: a) enable customers to conclude contracts for the supply of goods, services or digital	Chapter 1 Article 2 ➢ *Platform* is an information society service which provides one or more of the services set out in Article 1(2). ➢ *Platform* operator is a trader who operates a platform ➢ *Customer* is any natural or legal person who uses a platform for searching for or obtaining goods, services or digital content ➢ *Supplier* is any natural or legal person who uses a platform for marketing goods, services or

[383] See Directive (EU) 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 L 88, 31.3.2017, p. 6–21

[384] See European Law Institute (2019). Model Rules on Online Platforms.

Instrument	Scope of application	Definitions and references to online platforms
	content with suppliers within a digital environment controlled by the platform operator b) enable suppliers to place advertisements within a digital environment controlled by the platform operator which can be browsed by customers to contact suppliers and to conclude a contract outside the platform; c) offer comparisons/other advisory services to customers which identify relevant suppliers of goods, services or digital content and which direct customers to those suppliers' websites or provide contact details; d) enable platform users to provide reviews regarding suppliers, customers, goods, services or digital content offered by suppliers, through a reputation system.3. These rules are not intended to be used in relation to platforms operated in the exercise of public authority. ➢ Provisions for specific sectors, such as financial services, including insurance, or package travel and linked travel arrangements, take precedence to the extent that they deviate from these rules	digital content to customers/who has been suggested to customers by a platform; ➢ *Supplier-customer contract* is a contract under which goods/services/digital content are to be provided by a supplier to a customer against the payment of a price in money/any other counter-performance/in exchange for data ➢ *Platform-customer contract* is a contract concluded between a platform operator and a customer on the use of a platform ➢ *Platform-supplier contract* is a contract concluded between a platform operator and a supplier on the use of a platform ➢ *Consumer* is any natural person who, in contracts covered by these rules, is acting for purposes outside his or her trade, business, craft or profession ➢ *Trader* is any natural person or legal person, irrespective of whether privately or publicly owned, who is acting for purposes relating to its trade, business, craft or profession in relation to contracts covered by these rules ➢ *Platform user* is a supplier, a customer or a person who provides a review
	➢ This report focuses on online entities that serve at least two different sets of users simultaneously, bringing them together and enabling interactions between them that can benefit the users as well as the platform itself.	Other definition provided: ➢ *Stock exchanges* are platforms on which the users' interactions flow in two directions. The exchanges serve both stock buyers and stock sellers. They interact through the exchange by signaling the prices at which they are willing to buy and sell. Of course, both newspapers and stock exchanges have evolved into online platforms, too. ➢ *Video-sharing services* are platforms that can have at least three sets of users who interact in multiple directions: those who upload videos, those who watch them, and those who pay the platform to place advertisements. Interactions flow from video uploaders and advertisers to video consumers, but they also flow from consumers back to the uploaders

Instrument	Scope of application	Definitions and references to online platforms
		in the form of ratings and comments. In addition, they can flow from consumers to other consumers. ➢ *Online Platform* is a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet.
OECD: An Introduction to Online Platforms and Their Role in the Digital Transformation[385]	➢ The impetus for this report is the 2016 Cancún Ministerial Declaration on the Digital Economy, which contains a commitment to study online platforms. Ministers declared they would seize the opportunities made possible by online platforms that enable innovations in production, consumption, collaboration and sharing, while studying the platforms' social and economic benefits and challenges as well as the suitability of relevant policy and regulatory frameworks. That aspect of the Declaration is in line with recent comments from the United States business community urging that policy makers should try to better understand the benefits and potential issues that arise in the context of the ongoing platform growth. This report, moreover, is an output under the OECD's Going Digital horizontal project.	The term 'online platforms': ➢ The term '*online platform*' is used to describe a range of services available on the Internet including marketplaces, search engines, social media, creative content outlets, app stores, communications services, payment systems, services comprising the so-called 'collaborative' or 'gig' economy, and much more. An online platform is defined as a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet. The notion of platforms does not cover:Cloud services providers for they serve only one set of users traditional radio stations before the advent of streaming, for they served two sets of users (listeners and advertisers), but they were not online.

[385] See OECD (2019). An Introduction to Online Platforms.

Annex 3 - Regulatory frameworks

1. Commerce Directive

Legislative Framework

Directive 2000/31/EC on electronic commerce in the EU. Home Control Principle and Liability exemptions. At EU level, the general framework for online platforms' liability is to be found in the E-Commerce Directive 2000/31 (ECD).[386] The so called 'e-Commerce Directive' sets standard harmonised rules on various issues related to electronic commerce. Most importantly, it establishes the 'country of origin/home control principle' according to which OPs are subjects to the legal requirements of their Member States of establishment, and under Article 12 -15 it harmonises the conditions under which certain 'information society service providers' – those providing conduit, cashing and hosting of information at the request of third parties – benefit from the exemption of liability for the illegal content hosted by them (so called 'Safe Harbour'). In particular:

- Pursuant to Article 12, where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network (*mere conduit),* Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. This also applies in case of automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
- Pursuant to Article 13, where the service offered by the ISSP consists in the transmission in a communication network of information provided by a recipient of the service (*cashing),* Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that the provider (a) does not modify the information; (b) complies with conditions on access to the information; (c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
- Pursuant to Article 14, when the providers' service consists of the storage of information provided by a recipient of the service – who is not acting under the authority or control of the provider – (*hosting),* Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that the former (a) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

This 'Safe Harbour Regime' is of horizontal and general applications, thus excluding intermediaries from a wide range of liabilities – criminal, administrative and civil – for all the activities carried out by third parties through their platforms, provided that the conditions recalled above are met. In this sense, it excludes them from secondary liability, unless a series of duties of care established therein are not complied with (e.g. prompt removal of the information upon knowledge of its illegal nature). However, as indicated below, sectoral legislations have been adopted, which – despite not affecting the regime of secondary liability exclusion just described – complement it with a wide range of additional duties of care, creating parallel regimes of rights and duties depending on the type of infringement involved.

Furthermore, Article 15 states that under national law, ISSPs might hold a duty to promptly inform public authorities of alleged illegal activities undertaken or information provided by recipients of their service, and to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements. However, such obligation cannot consist in a general duty to monitor the content of the information transmitted or stored.

Soft law

Commission Recommendation on tackling illegal content online. In March 2018 the Commission proposed a series of measures to be adopted by Member States and online platforms to ensure quick and proactive detection, removal and

[386] See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

prevention of reappearance of illegal content, to be defined according to the 'what is illegal offline is illegal online' principle.[387] Those measures consist in:

- *Clearer 'NTD action' procedures.* OPs were asked to provide easy and transparent rules for notifying illegal content and fast-track procedures for 'trusted flaggers'. At the same time, they were asked to inform content providers and give them the opportunity to contest the action, eventually avoiding the removal of licit content.
- *More efficient tools and proactive technologies.* OPs were asked to provide clear notification systems, as well as proactive tools for the detection and removal of illegal content, in particular in cases of terrorism and child sexual abuse, counterfeited goods and – in general – of content which is potentially highly harmful and does not require contextualisation to qualify as illegal.
- *Stronger safeguards to ensure fundamental rights.* OPs were requested to put in place effective and appropriate safeguards, including human oversight and verification where automated tools and filters are used, to ensure that decisions to remove content are accurate, well-founded and fully respectful of fundamental rights, (freedom of expression, privacy and data protection in particular).
- *Closer cooperation with authorities.* Online platforms were asked to promptly inform law enforcement authorities upon evidence of a serious criminal offence, or reasons to suspect threat to life or safety of users or third parties, deriving from the illegal content present on their infrastructure or service.
- *Special attention to small companies.* Finally, the recommendation advocated for the adoption of voluntary arrangements, tools for sharing experiences and best practices, as well as technological solutions, including those enabling automatic detection, with the aim of benefitting smaller platforms, which may lack the necessary resources and experiences to adopt a higher degree of governance for tackling illegal content online.
- However, and most importantly, the adoption of all these measures was expressly stated as not affecting the liability regime set out in ECD (Article 12-15 ECD).

2. Media Law

Legislative Framework

The Audiovisual Media Services Directive (AVMSD). The AVMSD was originally adopted in 2010[388] to create and ensure the proper functioning of a single EU market for audiovisual media services. It was aimed at shaping technological developments, create a level playing field for emerging audiovisual media, promote cultural diversity, protect children and consumers, safeguard media pluralism, combat racial and religious hatred and guaranteeing the independence of national media regulators.

As part of the Digital Single Market Strategy, the original directive was amended and updated by Directive (EU) 2018/1808,[389] which modifies the regulatory framework as to make restriction directed to TV more flexible, strengthen the protection of European content, increase the effectiveness of measures for children protection and against hate speech, reinforce interdependence of national regulatory authorities, and –– extend certain audiovisual rules to video-sharing platforms as well as audiovisual content shared on certain social media services.

The AVMSD sets some fundamental principles for regulating audiovisual media services at European level and covers all services with audiovisual content irrespective of the technology used to deliver the content (principle of technological neutrality). It thus addresses both traditional TV broadcasts, on-demand audiovisual media services (AVMS). Furthermore, the directive also sets specific rules for video-sharing platform service (VSPS), which are defined as a service offering 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, using electronic communications networks, and the organisation of which is determined by the video-sharing platform provider, including by use of automatic means or algorithms, in particular by displaying, tagging and sequencing.

The AVMSD sets up rules on the:

- Freedom of reception, the 'country of origin principle', and the possibility for Member States to restrict reception of certain content that may not be banned in its country of origin but violates local laws, under the Commission's approval and in exceptional circumstances;
- Commercial communication, audiovisual advertising, sponsorship, and product placement;
- Protection of children. Pursuant to Article 6a and 28b Member States must take action to ensure that programmes which could 'impair the physical, mental or moral development of minors' are only made available in such a way that minors will not normally hear or see them, through selecting an appropriate time for broadcast,

[387] See C(2018) 1177 final.

[388] See Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), *OJ L 95, 15.4.2010, p. 1–24.*

[389] See Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, *OJ L 303, 28.11.2018, p. 69–92.*

age verification tools or other technical measures proportionate to the potential harm. The most harmful content, such as gratuitous violence and pornography, is subject to the strictest measures. Product placement is also prohibited in children's programming. EU countries should encourage the use of self- and co-regulation through codes of conduct regarding inappropriate advertising in children's programmes, for foods and beverages high in fat, salt and sugar.

- Prohibition of incitement to violence or hatred towards discriminated groups. AVMS must not contain incitement to violence or hatred directed against groups or a member of a group based on discrimination on grounds such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age, sexual orientation or nationality, in accordance with Article 21 of the EU Charter of Fundamental Rights.
- Prohibition of public provocation to commit a terrorist offence;
- Improved access for persons with disabilities;
- *Contact points*. EU countries must designate an online point of contact to provide information and receive complaints regarding accessibility issues. Public emergency information provided through audiovisual media services, for example in natural disaster situations, must be accessible to persons with disabilities.

***Rules applicable to VSPS*.** In reference to VSPS, Article 28b of the revised directive requires Member States put in place appropriate measures to:

- protect minors from programmes, user-generated videos and audiovisual commercial communications which could affect their physical, mental or moral development
- protect the general public from programmes, user-generated videos and audiovisual commercial communications containing:
- provocation to commit a terrorist offence, offences concerning child pornography and offences concerning racism and xenophobia;
- incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter of Fundamental Rights of the European Union.

Such measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the VSPS providers and the users having created or uploaded the content as well as the general public interest. Indeed, those measures shall be practicable and proportionate, taking into account the size of the video-sharing platform service and the nature of the service that is provided, and shall not lead to any ex-ante control measures or upload-filtering of content which do not comply with Article 15 ECD.

As per Article 28b (3) AVMSD, such measures shall include, among others, mechanisms and tools for: '

- '(e) establishing and operating systems through which video-sharing platform providers explain to users of video-sharing platforms what effect has been given to the reporting and flagging referred to in point (d);
- (f) establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors;
- (g) establishing and operating easy-to-use systems allowing users of video-sharing platforms to rate the content referred to in paragraph 1;
- (h) providing for parental control systems that are under the control of the end-user with respect to content which may impair the physical, mental or moral development of minors;
- (i) establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints to the video-sharing platform provider in relation to the implementation of the measures referred to in points (d) to (h);
- (j) providing for effective media literacy measures and tools and raising users' awareness of those measures and tools'.

Furthermore, the directive requires Member States to extend to VSPS providers the same obligations as audiovisual service providers in respect of advertising and other content restrictions, taking into account the limited control they can exercise over advertising on their platforms that is not marketed, sold or arranged by them.

Moreover, the directive requires Member States to ensure that VSPS apply those measures within their jurisdiction, and strongly encourage the adoption of co-regulatory instruments and exchange practices for fighting online content.

3. Online piracy, IP and copyrights infringements

Legislative framework

Directive 2019/790 on Copyright and related rights in the Digital Single Market. Directive 2019/790[390] sets important updates to the directives constituting the IP law framework[391], to adapt certain key exceptions to copyright to the digital and the cross-border environment, improve licensing practices and ensure wider access to content, and achieve a well-functioning marketplace for copyright. In particular, it introduces new mandatory exceptions allowing the use of copyright-protected material, fostering text- and data-mining and digital uses of works for the purpose of illustration for teaching and the preservation of cultural heritage. It then facilitates licensing to give wider access to content, in particular by providing a new system for cultural heritage institutions to digitalise and disseminate – also online and across borders in the EU – out-of-commerce works in their collections. It sets a rule on extended collective licensing, and a negotiation mechanism for making audio-visual works available on video-on-demand platforms.

The directive also grants new rights to EU-based press publishers working through online service providers for the digital use of their press publications, while requiring that authors of works included in a press publication receive an appropriate share of the income derived from its use.

Also, the directive prescribes that online content-sharing service providers should obtain permission from rightsholders to make works uploaded by their users available to the public, for example through a licensing agreement. If a licence is not concluded, the concerned platforms benefit from a liability-mitigation mechanism, but they have to make 'best efforts' to make sure that unauthorised content is not available on their websites. They must make those efforts since relevant and necessary information provided by the rightholders. Users can post content for the specific purposes of quotation, criticism, review, caricature, parody or pastiche and may use complaint and redress mechanisms in case of disputes over content erroneously blocked or removed from the platforms.

EU countries should ensure that a principle of appropriate and proportionate remuneration applies when an author or performer has transferred or licensed his rights for exploitation by another party (e.g. a publisher or a producer).

Also, authors and performers should receive regularly — at least once a year — up-to-date, relevant and comprehensive information on the exploitation of their works and performances. They have a right of revocation, after a reasonable period of time, in the event of non-use of the work or performance.

The negotiating rights of authors and performers are strengthened. They have the right to claim from the party with whom they have a contract for the exploitation of rights, appropriate and fair additional remuneration in cases where the remuneration initially agreed is unreasonably low in relation to all subsequent income resulting from exploitation of the works.

Intermediary liability – injunctions. The Directive 2004/48/EC on the enforcement of intellectual property rights (IPRED)[392] aims at providing a level playing field on the enforcement of IP rights, while the Directive 2001/29/EC aims to adapt legislation on copyright and related rights to technological developments, and particularly to the information society (Infosoc),[393] and both enact important mechanisms for the protection of IP rights against infringements online. The IPRED prescribes a minimum set of measures, procedures and remedies to ensure effective civil enforcement of intellectual property rights across Europe, tackling both piracy and counterfeit. By doing so, it also purses the promotion of innovation and business competitiveness, the safeguard of employment in Europe, respect of public order and consumer protection. In particular, it ensures that consumers are not mislead about products' safety and security and are not deprived of guarantees, after-sales service or effective remedies in case of damage. Under this directive, Member States are called to take appropriate action against those responsible for counterfeiting and piracy and to set up effective, proportionate and dissuasive measures, procedures and remedies needed to ensure the enforcement IPRs, without creating barriers to legitimate trade and offering safeguards against their abuse.

Article 9 (1) a) of the IPRED provides that judicial authorities may issue interlocutory injunctions against an intermediary whose services are used by a third-party to infringe such rights. Article 8(3) of the Infosoc, instead, provides that injunctions may be issued against an intermediary whose services are being used by a third party to infringe IP rights aimed at prohibiting the continuation of the infringement.

Precautionary seizure and corrective measures for recalling, removing, or destructing infringing goods are also allowed. Specific rules are also prescribed for calculating damages to compensate the injured party.

Sectoral legislation

[390] Directive (EU)2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, pp. 92-125)

[391] In particular: Directive 2001/29/EC on the harmonisation of copyright in the information society; and the directives on: the enforcement of intellectual property rights (Directive 2004/48/EC); orphan works (Directive 2012/28/EU); and the collective management of copyright and related rights (Directive 2014/26/EU).

[392] See Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157, 30.4.2004, p. 45–86.

[393] See 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, *OJ L 167 22.6.2001, p. 10–19.*

The Falsified Medicine Directive 2011/62/EU[394]**.** Online marketplaces exist also for medicine products. These marketplaces may distribute the medicine, or they may operate as intermediaries between online pharmacies and consumers. To tackle the illegal online sales of medicines in the EU, the Commission adopted the Falsified Medicine Directive 2011/62/EU. The Directive provides under Article 85c (1) (a) that, 'Member States shall ensure that medicinal products are offered for sale at a distance to the public by means of information society services' only under certain conditions to be complied with by the offeror of the medicinal products such as:

- authorisation of the offeror to supply the medicinal products to the public and at a distance;
- provision of information by the offeror to the Member States in question on the name or corporate name and permanent address of the place of activity from where those medicinal products are supplied and of the starting date of the activity of offering medicinal products for sale at a distance to the public by means of information society services and of the address of the website used for that purpose and all relevant information necessary to identify that website.

The Directive also imposes direct legal obligations on websites (including information society services providers although no express reference is made in the Directive in this respect) 'without prejudice to the information requirements set out in Directive 2000/31/EC'. As set forth in Article 85c (1) d), the websites offering the medicinal products are required to indicate contact details of the national authority notified by the offeror of medicinal products as indicated before, a hyperlink to the website of the offeror and a common logo clearly displayed on every page of the website that relates to the offer for sale at a distance to the public of medicinal products that contains in turn a hyperlink to the website of the national competent authority listing all persons offering the medicinal products for sale at a distance to the public by means of information society services.

Voluntary initiatives and codes of conducts

Ad-funded IP infringement. On June 2016, under the EC's aegis, a group of advertisers, advertising agencies, trading desks, advertising platforms, advertising networks, advertising exchanges, publishers and IP rights owners to the signing of the Memorandum of Understanding on online advertising and intellectual property rights[395] (MoU) to minimise the placement of advertising on websites and mobiles apps that infringe copyright or disseminate counterfeit goods. On the basis of their individual policies and assessment criteria, signatories should 'limit the placement of advertising on other websites and/or mobile applications, which have no substantial legitimate uses and for which advertisers have reasonably available evidence that these websites and applications are infringing copy-right or disseminating counterfeit goods on a commercial scale. Moreover, the MoU sets forth particular obligations for advertising Intermediaries, requiring them to:

- make sure that their contractual terms allow for the use of tools for content verification, advertising delivery and reporting so that advertising is not placed on IP rights infringing websites;
- take reasonable steps for the removal of such ads once identified;
- adopt IP rights policies describing the tool and measures adopted for complying with the MoU;
- report annually to the Commission and other signatories on the steps undertaken to comply with the MoU and their effectiveness.

Sale of counterfeit goods in online marketplaces. In 2011 major online platforms, associations and rights holders, with the facilitation of the European Commission, signed the Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet[396] (MoU) as a voluntary tool meant to prevent offers of counterfeit goods from appearing in online marketplaces by improving NTD measures and proactive measures. The MoU was revised and signed again in 2016 to include key performance indicators for tracking and measuring the MoU's success. The European Commission published so far three reports on the implementation of the MoU. The latest report shows that the MoU is a useful and efficient tool in counteracting the sale of counterfeit goods on the internet and that 'voluntary cooperation can provide the flexibility to discuss and deliver efficient solutions', although certain drawbacks have been reported by the signatories, other than online platforms such as[397] : (i) 'signatories consider the cooperation and information exchange with online platforms to fall short of the commitments made under the MoU' and (ii) 'signatories questioned the usefulness of directly comparing quantitative data provided through the KPI windows seeing the dynamics of the collection exercise, differences in methodology and the lack of reliable auditing'. Moreover, in June 2020 three rights owners in the fashion and luxury goods sectors decided to withdraw from the MoU, as they believe that progress is not sufficient, and the level of counterfeit offers is still too high. Overall, the conclusion is that although the MoU has provided certain benefits, its effectiveness is impacted by the low number of OPs signatories and sometimes their lack of involvement, and that future actions should not focus on the text of MoU but on how attract a higher degree of involvement and action.

[394] See Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products, OJ L 174, 1.7.2011, p. 74–87.

[395] See (2018). Memorandum of Understanding on online advertising and intellectual property rights.

[396] See (2011). The Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet.

[397] See SWD(2020) 166 final/2., pp. 37-38.

4. Child Protection

Legislative framework
Regulatory Framework – Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography. Directive 2011/93[398] obliges Member States to adopt preventive measures against sexual abuse and sexual exploitation of children and child pornography, to protect child victims, as well as to investigate and prosecute offenders. Most importantly, the directive requires them to ensure the prompt removal of web pages containing or disseminating child pornography in their territory, and to work to obtain removal if hosted outside their jurisdiction, also allowing blocking measure to prevent abuse. According to Article 25, these measures may be of legislative or non-legislative nature, as long as they are adequate for the attainment of the goals set therein. They must be set by transparent procedures and provide adequate safeguards, ensuring that restrictions are necessary and proportionate, that users are informed of the reason for the restriction, and that the possibility of judicial redress is granted.
Soft law and voluntary initiatives
The European Strategy for a Better Internet for Children.[399] The European Strategy for a Better Internet for Children connects EU Institutions, Member States, and industry (e.g. mobile phone operators, handset manufacturers and providers of social networking services). It aims at ensuring ➢ *High quality content online for children and young people*, by: (i) stimulating the production of creative and educational online content for children, and (ii) promoting positive online experiences for them; ➢ *Stepping up awareness and empowerment*, through: (i) digital literacy and online safety in all EU schools, (ii) scaling up awareness activities in youth participation, (iii) simple and robust reporting tools for users; ➢ *Creating a safe environment for children online*, through: (i) age-appropriate privacy settings, (ii) wider availability and use of parental controls; (iii) wider use of age rating and content classification; (iv) online advertising and overspending; ➢ *Combatting child sexual abuse material online and child sexual exploitation*, through: (i) faster and systematic identification of child sexual abuse material disseminated through various channels, notification and takedown of this material; (ii) cooperating with international partners to fight against child sexual abuse and child sexual exploitation.
Safer Internet Centres. The Commission co-funds Safer Internet Centres in Member States (coordinated by Insafe), with the Better Internet for Kids portal as a single entry point for resources and sharing best practices across Europe. Their main task is to raise awareness and foster digital literacy among minors, parents and teachers. They also fight against online child sexual abuse material through its network of hotlines (INHOPE).
Alliance to better protect minors online. The Alliance to better protect minors online is a self-regulatory initiative supported by the Commission and featuring leading ICT and media companies, civil society and industry associations tackling harmful online content and behaviour, including harmful content, harmful conduct and harmful contact which children may experience online. The members of the Alliance adopted commitments and signed a common Statement of purpose[400], which sets three main goals: ➢ *user-empowerment* through: (i) identification and promotion of best practice for the communication of data privacy practices; (ii) accessible, robust and easy-to-use tools with appropriate feedback and notification systems; (iii) promotion of users' awareness to ensure self-safety and responsible and respectful behaviours towards others; (iv) promotion of content classification and (v) parental control tools; ➢ *enhanced collaboration with other parties to*: (i) enhance best practice-sharing; (ii) identifying emerging developments in technology: ➢ *awareness raising* through: (i campaigns about online safety, digital empowerment, and media literacy; (ii) promotion of children's access to diversified online content, opinions, information and knowledge. Due to the broadness of the Alliance's member base and the relative abstract-nature of the commitments, members are supposed to focus on those commitments that are directly relevant to the risks and concerns that are more relevant for their activity. Following the agreement made with the EU Commission, the work of the Alliance has been subject to evaluation through and independent reports[401].

[398] See Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities PE/33/2018/REV/1 *OJ L 303, 8.11.2018, p. 69–92.*

[399] See COM(2012) 196 final.

[400] See (2017). A Safer Internet for Minors.

[401] See https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/child-sexual-abuse/global-alliance-against-child-abuse_en.

Global Alliance against Child Sexual Abuse Online and the WeProtect Global Alliance.[402] By signing up to the Global Alliance Against Child Sexual Abuse Online – a joined EU and US initiative – 54 countries from around the world committed to key policy targets that aim at a larger number of rescued victims, more effective prosecution, and an overall reduction in the number of child sexual abuse images available online.
The Global Alliance the merged with other initiatives to form the WeProtect Global Alliance to end child sexual exploitation online, which rallies over 80 governments, 20 global technology companies and 24 leading international and non-governmental organisations to protect children from sexual exploitation online.

5. Hate Speech

Legislative Framework

Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law. The Framework Decision[403] aims to ensure that in all Member States serious manifestations of racism and xenophobia committed within the territory of the European Union, by a European national, or for the benefit of a legal person established within the EU, are punishable through effective, proportionate and dissuasive criminal penalties, and to foster judicial cooperation to this end.
In particular, it sets as punishable criminal offences a series of action related to hate speech, as well as their instigation, aiding or abating, namely:

- public incitement to violence or hatred directed against a group of persons or a member of such a group defined on the basis of race, colour, descent, religion or belief, or national or ethnic origin;
- the above-mentioned offence when carried out by the public dissemination or distribution of tracts, pictures or other material;
- publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes as defined in the Statute of the International Criminal Court and crimes defined in Article 6 of the Charter of the International Military Tribunal, when the conduct is carried out in a manner likely to incite violence or hatred against such a group or a member of such a group – as well as the aiding and abating and instigation of said offences).

AVMSD. Under the revised AVMSD, the authorities in every EU country must ensure that audiovisual media services do not contain any incitement to hatred based on race, sex, religion or nationality. This is an issue, for instance, with channels that endorse violence as the solution to social or political conflicts. Banning a television channel outright must remain a last resort to be balanced against the democratic right to free speech, as it is a radical move. In addition to corresponding national broadcasters, authorities in Member States are required to act against hate speech channels using an uplink in an EU country, and satellite capacity being used for hate speech broadcasts. EU authorities have no power under AVMSD to act against hate speech channels from outside the EU, such as outside satellite channels that can be picked up in parts of the EU. The Commission regularly raises the issue of hate speech broadcasters in its political dialogue with the countries concerned, particularly those where the broadcasters are based.

Moreover, under specific provisions for hate speech online set in the revised AVMSD (i.e. Article 28b (1) b), Member States must *ensure that video-sharing platforms adopt and implement appropriate measures to:*

- '*protect the general public* from programmes, user-generated videos and audiovisual commercial communications containing incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter i.e. 'sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation'; and
- '*protect the general public* from programmes, user-generated videos and audiovisual commercial communications containing incitement to racism and xenophobia'.

Soft law and voluntary initiatives

Code of Conduct on Countering Illegal Hate Speech Online. Against this background, in May 2016, the Commission agreed with certain OPs' representatives on a Code of conduct on countering illegal hate speech online, to prevent and counter the spread of illegal hate speech online.[404] The Code provides the following voluntary measures that signatories can implement, such as:

- introducing in their terms and conditions a prohibition against the promotion of incitement to violence and hateful conduct;

[402] See https://www.weprotect.org/our-mission-and-strategy.

[403] See Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, *OJ L 328, 6.12.2008, p. 55–58.*

[404] See The EU Code of conduct on countering illegal hate speech online 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

- adopting clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content and provide information on the procedures for submitting notices;
- reviewing the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content;
- encouraging the provision of notices and flagging of content that promotes incitement to violence and hateful conduct at scale by experts and making information about 'trusted reporters' available on their websites;
- providing regular training to their staff on current societal developments and to exchange views on the potential for further improvement and identifying and promoting independent counter-narratives, new ideas and initiatives and supporting educational programs that encourage critical thinking.

The implementation of the Code of Conduct is evaluated through a regular monitoring exercise set up in collaboration with a network of organisations located in the different EU countries. Using a commonly agreed methodology, these organisations test how the IT companies are implementing the commitments in the Code.

National legislation

France. France passed in November 2018 a new law against manipulation of information[405]. The law imposes on online platform specific obligations during the electoral process. In particular, platforms are required to:

- provide users with fair, clear and transparent information allowing the identification of the person/entity that pay the platform for promoting certain content, and the use of their personal data in the context of promoting information content related to a public interest debate;
- implement measures to combat the dissemination of false information that could disturb public order or impair sincerity, such as a mechanism easily accessible and visible that allows users to report such information, especially when it comes from content promoted on behalf of a third party, and complementary measures such as transparency of their algorithms, informing the users on the origin, nature and modalities to distribute content;
- publish aggregated statistics on the algorithms' functions, in case of algorithms-based promotion of content related to a debate of general interest, such as recommendation, ranking or referral of information.

In case of violation of said duties, online platforms may face pecuniary sanctions (a fine of EUR 75,000), as well an interdiction to exercise the activity related to the crime.

With specific reference to voting manipulation, the law prescribes that when inaccurate or misleading allegations or imputations of a fact likely to alter the sincerity of the election are deliberately, artificially or automated and massively disseminated through an online public communication service, the judge may, take any proportionate and necessary measures to stop this dissemination.

Germany. Germany passed on 1 October 2017 a law against fake news and hate crimes in social networks,[406] i.e. the Network Enforcement Act, also known as NetzDG. The following obligations are imposed on 'telemedia service providers which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public':

- 'manifestly unlawful content shall be removed within 24 hours of receiving the complaint, whereby a longer period of time for blocking or deletion can be agreed individually with the competent law enforcement authority';
- 'the access to other unlawful content shall be removed or blocked without delay and generally within seven days';
- 'the management of the social network shall monitor the established procedure via monthly checks and offer training courses and support programmes delivered in the German language on a regular basis to the persons tasked with the processing of complaints';
- 'providers of social networks which receive more than 100 complaints per calendar year about unlawful content shall be obliged to produce half-yearly German-language reports on the handling of complaints about unlawful content on their platforms and shall be obliged to publish these reports in the Federal Gazette and on their own website no later than one month after the half-year concerned has ended'.

[405] See *32 Loi n° 2018-1202 relative à la lutte contre la manipulation de l'information, 22 December 2018.* https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law

[406] Available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html.

6. Disinformation and voting manipulation

Legislative framework

The AVMSD. In 2018, the AVMSD has been reviewed as a new type of content online has emerged and it is being widely consumed such as video clips or user-generated content and also new players have emerged such as video-on-demand services and video-sharing platforms, including social media platforms. As per Recital 4 AVMSD, 'social media services need to be included in the scope of Directive 2010/13/EU because they compete for the same audiences and revenues as audiovisual media services. Furthermore, they also have a considerable impact in that they facilitate the possibility for users to shape and influence the opinions of other users. Therefore, in order to protect minors from harmful content and all citizens from incitement to hatred, violence and terrorism, those services should be covered by Directive 2010/13/EU to the extent that they meet the definition of a video-sharing platform service'. As per Article 28 (b), without prejudice to articles 12 to 15 of Directive 2000/31/EC, Member States shall ensure that video- sharing platform providers under their jurisdiction take appropriate measures to protect:

- minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1);
- the general public from programmes, user-generated videos and audiovisual commercial communications containing incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter.

In accordance with Article 9 and Art 28b (2) of the AVMSD, Member States shall ensure that audiovisual commercial communications marketed, sold or arranged by video sharing platforms under their jurisdiction comply with a series of requirements. In particular:

- audiovisual commercial communications shall be readily recognisable as such; surreptitious audiovisual commercial communication shall be prohibited;
- audiovisual commercial communications shall not use subliminal techniques;
- audiovisual commercial communications shall not: (i) prejudice respect for human dignity; (ii) include or promote any discrimination based on sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation; (iii) encourage behaviour prejudicial to health or safety; (iv) encourage behaviour grossly prejudicial to the protection of the environment.

Member States shall ensure that video-sharing platform providers clearly inform users where programmes and user-generated videos contain audiovisual commercial communications, provided that such communications are declared under point (c) of the third subparagraph of paragraph 3 or the provider has knowledge of that fact. For the purposes of paragraphs 1 and 2, the appropriate measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having created or uploaded the content as well as the general public interest.

Those measures shall consist of, as appropriate:

- including and applying in the terms and conditions of the video-sharing platform services the requirements referred to in paragraph 1;
- including and applying in the terms and conditions of the video-sharing platform services the requirements set out in Article 9(1) for audiovisual commercial communications that are not marketed, sold or arranged by the video-sharing platform providers;
- having a functionality for users who upload user-generated videos to declare whether such videos contain audiovisual commercial communications as far as they know or can be reasonably expected to know;
- establishing and operating transparent and user-friendly mechanisms for users of a video-sharing platform to report or flag to the video-sharing platform provider concerned the content referred to in paragraph 1 provided on its platform;
- establishing and operating systems through which video-sharing platform providers explain to users of video-sharing platforms what effect has been given to the reporting and flagging referred to in point (d);
- establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors;
- establishing and operating easy-to-use systems allowing users of video-sharing platforms to rate the content referred to in paragraph 1;
- providing for parental control systems that are under the control of the end-user with respect to content which may impair the physical, mental or moral development of minors;
- establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints to the video-sharing platform provider in relation to the implementation of the measures referred to in points (d) to (h);
- providing for effective media literacy measures and tools and raising users' awareness.

Soft law and voluntary initiatives

The Commission's Communication on Tackling online disinformation. The EU has made extensive efforts to tackle disinformation and voting manipulation. Following *inter alia* the scandal of the interference with the UK and US elections,

in its Resolution on online platforms and the digital single market,[407] the EU Parliament solicited the Commission for action. The latter set up a high-level expert group and a public consultation,[408] and in April 2018 released a Communication on Tackling online disinformation,[409] where it calls on Member States to put forward several tools to tackle the spread and impact of online disinformation and ensure the protection of EU values and democratic systems. In particular, these tools must aim at ensuring diversity and credibility of information, as well as transparency over the way it is produced or sponsored, and strive for inclusive solutions with broad stakeholder involvement. In particular, the Commission urged OPs to act swiftly and effectively to protect users from disinformation and to create a more transparent, trustworthy and accountable online ecosystem.

Following this line, the European Union has outlined an Action Plan to strengthen cooperation between Member States by (i) improving detection, analysis and exposure of disinformation; (ii) ensuring stronger cooperation and joint responses to threats; (iii) enhancing collaboration with OPs and industry to tackle disinformation, (iv) raising awareness and improve societal resilience.[410]

The Code of Practice on Disinformation. Urged by the Commission's call to develop an EU-based Code of Practice, representatives of online platforms, leading social networks, advertisers and advertising industry agreed on a self-regulatory Code of Practice to address the spread of online disinformation and fake news.[411] Under the Code, the signatories committed to four main goals:

- *scrutiny of ad-placements, political and 'issue-based' advertising*, to: (i) disrupt advertising and monetisation incentives for relevant behaviours; (ii) ensure that advertisements are clearly distinguishable from editorial content; (iii) enable public disclosure of political advertising; (iv) use reasonable efforts towards devising approaches to publicly disclose 'issue-based advertising';
- *integrity of services*, by: (i) putting in place clear policies regarding identity and the misuse of automated bots; (ii) putting in place policies on what constitutes impermissible use of automated systems, and to make this policy publicly available on the platform and accessible to EU users:
- *empowering users*, by: (i) helping people make informed decisions when they encounter online news that may be false, including by supporting efforts to develop and implement effective indicators of trustworthiness in collaboration with the news ecosystem; (ii) investing in technological means to prioritise relevant, authentic and authoritative information; (iii) investing in features and tools to make it easier to find diverse perspectives; (iv) support efforts aimed at improving critical thinking and digital media literacy; (v) encouraging market uptake of tools that help consumers understand why they are seeing particular advertisements;
- *empowering the research community*, by: (i) supporting good faith independent efforts to track and research disinformation and political advertising, including the independent network of fact-checkers facilitated by the European Commission; (ii) convening an annual event to foster discussions within academia, the fact-checking community and members of the value chain.

The entire range of commitments does not apply to all signatories, who shall rather identify those that correspond to the product and service they offer and/or their technical capabilities. Also, the measures for implementation were to be decided by the signatories and declared and explained in an annual report publicly available.

National regulation

France. Efforts in combatting disinformation and voting manipulation were also made at the national level. France passed in November 2018 a new law against manipulation of information.[412] The law imposes on OPs specific obligations during the electoral process. In particular, platforms are required to: (i) provide users with fair, clear and transparent information allowing the identification of the person/entity that pays the platform for promoting certain content, and the use of their personal data in the context of promoting information content related to a public interest debate; (ii) implement measures to combat the dissemination of false information that could disturb public order or impair sincerity, such as a mechanism easily accessible and visible that allows users to report such information, especially when it comes from content promoted on behalf of a third party, and complementary measures such as transparency of their algorithms, informing the users on the origin, nature and modalities to distribute content; (iii) publish aggregated statistics on the algorithms' functions, in case of algorithms-based promotion of content related to a debate of general interest, such as recommendation, ranking or referral of information. In case of violation of said duties, online platforms may face pecuniary sanctions (a fine of EUR 75,000), as well an interdiction to exercise the activity related to the crime. With specific reference to voting manipulation,

[407] See European Parliament (2017). Resolution on online platforms and the digital single market (2016/2276(INI)).

[408] See Synopsis Report of the European Commission of 26 April 2018 of the public consultation on fake news and online disinformation, available at: https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-fake-news-and-online-disinformation. Also see Flash Eurobarometer 464 (2018). Report on Fake news and disinformation online.

[409] See COM(2018) 236 final. Also see JOIN (2018) 36 final.

[410] See COM(2018) 236 final.COM(2018) 236 final.COM(2018) 236 final.COM(2018) 236 final.COM(2018) 236 final.COM(2018) 236 final.COM(2018) 236 final.COM(2018) 236 final., p. 5 ff.

[411] See (2018). Code of Practice on Disinformation. With regards to the online platforms signatories, Facebook, Google, Twitter and Mozilla subscribed to the Code on October 2018, Microsoft on May 2019 and TikTok in June 2020. See https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[412] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information available at https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000037151987/.

the law prescribes that when inaccurate or misleading allegations or imputations of a fact likely to alter the sincerity of the election are deliberately, artificially or automated and massively disseminated through an online public communication service, the judge may, take any proportionate and necessary measures to stop this dissemination.

Germany. Germany passed on 1 October 2017 a law against fake news and hate crimes in social networks[413], i.e. the Network Enforcement Act, also known as NetzDG, obliging social networks to remove manifestly unlawful content within 24 hours since receiving the complaint, whereby a longer period of time for blocking or deletion can be agreed individually with the competent law enforcement authority, and to remove or block access to other unlawful content without delay and generally within seven days. Moreover, the social network shall monitor the established procedure via monthly checks and offer training courses and support programmes delivered in the German language on a regular basis to the persons tasked with the processing of complaints. Those providers of social networks which receive more than unlawful-content related 100 complaints per year shall produce every 6 months reports on the handling of complaints, and publish them in the Federal Gazette and on their own website. Sanctions are with fines of up to 5 mil. EUR.

European Parliament resolution on foreign electoral interference and disinformation in national and European.[414] In its Resolution the European Parliament stated that the responsibility for countering disinformation and foreign electoral interferences lies not exclusively with public authorities but also with internet and social media companies, which should therefore cooperate in achieving this aim while not undermining freedom of speech or becoming privatised censorship bodies. Further, the European Parliament acknowledged the positive impact of the voluntary action taken by service providers and platforms to counter disinformation, including new rules to increase the transparency of electoral advertising on social media in the Code of Practice, as well as the measures implemented by the Commission and the Member States in the last year, and reminded them of their joint responsibility when it comes to the fight against disinformation. It also recalled its resolution of 25 October 2018, in which it urged Facebook, following the Cambridge Analytica scandal, to implement various measures to prevent the use of the social platform for electoral interference, and it notes that Facebook has not followed upon most of these requests. Moreover, it highlighted that these threats can neither be addressed solely by national authorities working in isolation nor by pure self-regulation of the private sector but require a coordinate multi-level, multi-stakeholder approach, and that a legal framework for tackling hybrid threats, including cyber-attacks and disinformation, should be developed both at EU and international level, in order to enable a robust response by the EU. Lastly, it called on the Commission to evaluate possible legislative and non-legislative actions which can result in intervention by social media platforms with the aim of systematically labelling content shared by bots, reviewing algorithms in order to make them as unbiased as possible, and closing down accounts of persons engaging in illegal activities aimed at the disruption of democratic processes or at instigating hate speech, while not compromising on freedom of expression.

7. Extremist and terrorist content

Legislative framework

Directive (EU) 2017/541 on combating terrorism. Directive 2017/541[415] aims to adapt EU law to fight terrorism in light of evolving terrorist threats and taking into account the international nature of terrorism and its reliance on online activities. It establishes minimum rules concerning the definitions of offences and related sanctions in this area, and introduces measures of protection, support, and assistance for victims. In particular, the directive provides an exhaustive list of serious offences that must be considered as terrorist offences when committed, or threated to be committed for a particular terrorist aim (i.e. seriously intimidating a population; unduly compelling a government or an international organisation to perform or abstain from performing any act; seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation), and extends criminal punishment to cover offences related to a terrorist group (i.e. directing such a group or knowingly participating in its activities) when committed intentionally, and offences related to terrorist activities (including, for what interests us the most: distributing online or offline a message with the intention of inciting a terrorist offence; soliciting and recruiting another person to commit a terrorist offence; providing or receiving training for terrorist purposes, providing or collecting funds with the intention that they be used or in the knowledge that they be used to commit terrorist offences).

In addition to prescribing the adoption of rules on aiding and abetting, inciting and attempting, jurisdiction and prosecution, as well as penalties and sanctions for physical persons and legal entities liable for the offences, the directive requires Member States to: (i) take measures for the prompt removal of and blocking of access to online terrorist content hosted in their territory, (ii) to obtain the removal of such content hosted outside their territory; and (iii) to respect fundamental rights and fundamental legal principles, as enshrined in Article 6 TUE in the implementation of the directive.

[413] available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html.

[414] European Parliament (2019). Resolution on foreign electoral interference and disinformation in national and European democratic processes.

[415] See Directive (EU) 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 L 88, 31.3.2017, p. 6–21.

As per Recital 22: 'an effective means of combating terrorism on the internet is to remove online content constituting a public provocation to commit a terrorist offence at its source. Member States should use their best endeavours to cooperate with third countries in seeking to secure the removal of online content constituting a public provocation to commit a terrorist offence from servers within their territory. However, when removal of such content at its source is not feasible, mechanisms may also be put in place to block access from Union territory to such content. The measures undertaken by Member States in accordance with this Directive in order to remove online content constituting a public provocation to commit a terrorist offence or, where this is not feasible, block access to such content could be based on public action, such as legislative, non-legislative or judicial action. In that context, this Directive is without prejudice to voluntary action taken by the internet industry to prevent the misuse of its services or to any support for such action by Member States, such as detecting and flagging terrorist content. Whichever basis for action or method is chosen, Member States should ensure that it provides an adequate level of legal certainty and predictability for users and service providers and the possibility of judicial redress in accordance with national law. Any such measures must take account of the rights of the end users and comply with existing legal and judicial procedures and the Charter of Fundamental Rights of the European Union (the Charter)'.
Furthermore, Recital 23 states that 'the removal of online content constituting a public provocation to commit a terrorist offence or, where it is not feasible, the blocking of access to such content, in accordance with this Directive, should be without prejudice to the rules laid down in Directive 2000/31/EC of the European Parliament and of the Council. In particular, no general obligation should be imposed on service providers to monitor the information which they transmit or store, nor to actively seek out facts or circumstances indicating illegal activity. Furthermore, hosting service providers should not be held liable as long as they do not have actual knowledge of illegal activity or information and are not aware of the facts or circumstances from which the illegal activity or information is apparent'.
Measures against public provocation content online are provided under Article 21, namely:

- Member States shall take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence, as referred to in Article 5, that is hosted in their territory. They shall also endeavour to obtain the removal of such content hosted outside their territory.
- Member States may, when removal of the content referred to in paragraph 1 at its source is not feasible, take measures to block access to such content towards the internet users within their territory.
- Measures of removal and blocking must be set following transparent procedures and provide adequate safeguards, in particular to ensure that those measures are limited to what is necessary and proportionate and that users are informed of the reason for those measures. Safeguards relating to removal or blocking shall also include the possibility of judicial redress.

Revised Audiovisual Media Service Directive. To complement the rules set out in the Counter-terrorism directive, Member States are also required to ensure that VSP adopt appropriate and specific measures to protect the public the general public from programmes, user-generated videos and audiovisual commercial communications containing provocation to commit a terrorist offence, as indicated above.

Soft law instruments

Proposal Regulation on preventing the dissemination of terrorist content online. The EU Commission published a Proposal Regulation on preventing the dissemination of terrorist content online.[416] Once negotiations were opened, a series of concerned was expressed by, among other, members of the United Nation Human Rights Council and by the EU Fundamental Rights Agency. An amended version of the proposal was adopted on 17 April 2019.
At the present stage, the proposal defines terrorist content as 'material which incites or solicits the commission or contribution to the commission of terrorist offences, provides instructions for the commission of such offences or solicits the participation in activities of a terrorist group' and guides on how to produce and use explosives, firearms and other weapons for terrorist purposes, adopts the aforementioned one-hour rule and, most importantly, sets a duty of care for all platforms to ensure they are not misused for the dissemination of terrorist content. Furthermore, the proposal calls on platforms to take proactive measure to avoid terrorist abuse. In this line, it also prescribes the creation of mechanisms for cooperation among hosting service providers, Member States and Europol, requiring service providers and Member States to designate points of contact allowing follow up to removal orders and referrals. Finally, service providers are asked to put in place effective complaint mechanisms for content providers, and that unjustified removed content shall be reinstated as soon as possible. Likewise, Member States and platforms are asked to put in place effective judicial remedies to ensure content providers the right to challenge a removal order. In case of automated detection tools, service providers shall ensure human oversight and verification to prevent erroneous removals. As far as enforcement and compliance-checking mechanisms are concerned, the proposal sets up annual transparency reports, while service providers might face sanctions up to 4% of their global turnover if they systematically and persistently fail to abide by the legislation on terrorist content. However, no obligation to monitor or filter the content is set, despite the one-hour rule.[417]

[416] See COM(2018) 640 final.

[417] See Legislative Train Schedule of the action to prevent the dissemination of terrorist content online available: https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-preventing-the-dissemination-of-terrorist-content-online and the Ordinary legislative procedure 2018/0331(COD) on Preventing the dissemination of terrorist content online available at https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2018/0331(COD).

Cooperative Bodies and Initiatives – EU Internet Forum.[418] The EU Internet Forum is a key commitment set with the Commission's European Agenda on Security 2015, and constitutes and institutional setting where EU Interior Ministers, high-level representatives of the major OPs, Europol, the EU Parliament and the EU Counter-terrorism coordinator work together with the aims to provide a framework for an efficient cooperation with the internet industry in the future, and to secure a commitment from the main actors to coordinate and scale up efforts in this area in the coming years. Against this background, the Internet Forum's goal is to prevent and fight online terrorist content, working on cooperation and exchange of information – such as the Europol's EU Internet Referral Unit, a vast database containing hashes of terrorist material removed from the Internet – and monitoring initiatives and progress in the online fight to terrorism, in particular with regard to the use and efficacy of automated flagging and removal systems.

8. Unsafe Products

Legislative framework

Product Liability Directive (PLD).[419] Under Article 1 the PLD sets forth a strict liability regime i.e. liability without fault, mainly on the producer of a product for damages caused by the product to the injured person. The same liability applies to importers of goods in the EU for 'for sale, hire, leasing or any form of distribution in the course of his business'. Under Article (3), the PLD extends liability also to suppliers which shall be treated as producers when either: (i) the producer of the product cannot be identified and the supplier fails to inform the injured person, within a reasonable time, of the identity of the producer or of the person who supplied him with the product, or (ii) in the case of an imported product, if this product does not indicate the identity of the importer, even if the name of the producer is indicated.
As stated in Article (3) of the PLD, the supplier will be deemed as a producer if it fails, within a reasonable time to provide the information on producer's identity. The 'reasonable time' period is an element that was left for the Member States to decide. In Sweden and Germany such a period is equal to one month, whereas in Italy such duration is equal to 3 months. Furthermore, in order to activate a supplier's liability, the victim is 'obliged to notify the supplier formally, so that he can within a reasonable time provide details of the producer or previous supplier'.[420]
The rationale for this provision is for consumers to easily find a liable person. Nevertheless, it should be noted that the suppliers' liability is a subsidiary liability which applies only to the extent the actual producer cannot be identified. Therefore, 'apart from the limited instances referred to the liability of professionals acting as simple suppliers is not governed by the provisions of Directive 85/374/EEC', and in order to invoke the possible liability of the supplier, the victim of the damage caused by the defective product must use the system governing liability laid down in the legislation of the Member State in question.
The term 'supplier is not defined in the PLD. The CJEU stated that a supplier is an 'operator in the production and marketing chain'.[421] Thus, 'the supplier must be regarded as any intermediary involved in the marketing or distribution chain of the product'.[422]

The Regulation on market surveillance[423]**.** The Regulation lays down rules and procedures for economic operators regarding products subject to certain Union harmonisation legislation listed in Annex 1 of the Regulation and establishes a framework for cooperation between economic operators, market surveillance authorities and other authorities. The Regulation also provides for market surveillance authorities' specific obligations and power do adopt and impose measures to ensure that the products are compliant with the existing legislation.
With respect to the area of products sold online and online platforms' obligations with respect to the latter, the Regulation provides for the following direct legal obligations incumbent upon information society services providers:

- an obligation to cooperate with the market surveillance authorities, at the request of the market surveillance authorities;
- in specific cases, to facilitate any action taken to eliminate the risks presented by a product that is or was offered for sale online through their services; or
- if that is not possible, to mitigate the risks presented by a product that is or was offered for sale online through their services.

[418] The EU Internet Forum's Statutes and Bylaws are available at https://www.internetforum.eu/about/about-us.html.

[419] See Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985, p. 29–33.

[420] European Commission (1996). Green Paper Liability for defective products. COM(1999)396 final Brussels, European Commission.

[421] See Case C-495/10, Centre hospitalier universitaire de Besançon v Thomas Dutrueux and Caisse primaire d'assurance maladie du Jura, EU:C:2011:869, para 26-28.

[422] See European Commission (2018). Commission Staff Working Document. Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. SWD(2018) 157 final Brussels, European Commission. , p. 105.

[423] See Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, PE/45/2019/REV/1, OJ L 169, 25.6.2019, p. 1–44.

These obligations have all as a condition precedent an act or measure imposed by market surveillance authorities or any other authorities. The thresholds and specific means for complying with such obligations are not set forth in the Regulation and their interpretation will be most likely further clarified through case-law and guidelines issued by the Commission in accordance with Article 33 (n) of the Regulation or by national authorities.
The Regulation also provides that the market surveillance authorities have, as a last resort (Article 14 (4) k) the right to request information society services providers to:

- first, remove the content referring to the related products from an online interface or require the explicit display of a warning to end users when they access an online interface;
- or, where a request according to the first point has not been complied with, to require information society service providers to restrict access to the online interface, including by requesting a relevant third party to implement such measures.

As per Recital 41, these measures may be imposed only 'where duly justified and proportionate and where there are no other means available to prevent or mitigate such harm, including, where necessary, requiring the removal of content from the online interface or the display of a warning' and provided such a request is not observed by the online interface. These measures consecrate at EU level the so called 'notice and action' procedure. The aforementioned measures shall not conflict with the principles laid down in the ECD, 'in particular, no general obligation should be imposed on information society service providers to monitor the information which they transmit or store, nor should a general obligation be imposed upon them to actively seek facts or circumstances indicating illegal activity.
Failure to comply with such measures will be sanctioned in accordance with the national law of the Member States and the nature of such sanctions could be administrative or criminal fines for failure to comply with an administrative order. The penalties for infringement of the Regulation will be laid down in national law by the Member States.

The Toy Directive.[424] The Directive imposes certain obligations with respect to the warning labels and instructions toys shall bear. In accordance with Article 11 (2), warnings which determine the decision to purchase the toy shall appear on the consumer packaging or be otherwise clearly visible to the consumer before the purchase, including in cases where the purchase is made on-line, such as the 'not suitable for children under 3' warning. These obligations are incumbent upon manufacturers, importers and distributors and they do not extend to online marketplaces for example, although more often than not such marketplaces are being used for the purchase of toys as a one-stop-shop through which consumers gather all the product information displayed on the marketplace, analyse reviews and order the product.

Regulation 2019/1148 on the marketing and use of explosive precursors,[425]. The Regulation establishes harmonised rules concerning the making available, introduction, possession and use of substances or mixtures that could be misused for the illicit manufacture of explosives, with a view to limiting the availability of those substances or mixtures to members of the general public, and with a view to ensuring the appropriate reporting of suspicious transactions throughout the supply chain. It imposes on online marketplaces obligations aligned to the emerging role of online platforms as 'educators' of their users, such as the obligation to take measures to ensure that its users, when making available regulated explosives precursors through their services, are informed of their obligations under the Regulation.
Also, online marketplaces have the obligation to deploy the necessary measures for allowing economic operators compliance with their obligations related to the verification of the identity of the buyer, the right to acquire explosive precursors and their intended use. Furthermore, for the purpose of this Regulation, online platforms are set on an equal foot with economic operators with respect to certain obligations for the purpose of preventing and detecting the illicit manufacture of explosives such as: (i) reporting of suspicions transactions and reporting of refused suspicious transactions; (ii) implementation of appropriate, reasonable and proportionate procedures to detect suspicious transactions; (ii) cooperation with the national authorities, economic operators, law enforcement authorities and representatives of the explosives sector.
The Regulation clarifies that the obligations imposed 'shall not amount to a general monitoring obligation'. Thus, the Regulation, together with the Guidelines to be issued by the Commission based on the Regulation 'should lay down only specific obligations for online marketplaces with respect to the detection and reporting of suspicious transactions that take place on their websites or that use their computing services'. Furthermore, 'online marketplaces should not be held liable, on the basis of this Regulation, for transactions that were not detected despite the online marketplace having in place appropriate, reasonable and proportionate procedures to detect such suspicious transactions'. Therefore, the Regulation imposes a specific duty of care on online marketplaces.

Soft-law and Voluntary Initiatives

Product Safety Pledge. On June 2018, four major online marketplaces signed the Product Safety Pledge[426] through the facilitation of the European Commission and thus voluntarily committed to undertake certain obligations and implement certain actions concerning consumer non-food unsafe products sold online by third parties on their marketplaces. The

[424] See Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys, OJ L 170, 30.6.2009, p. 1–37

[425] See Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013, OJ L 186, 11.7.2019, p. 1–20.

[426] See (2020). Product Safety Pledge. Also see European Commission Product safety rules. How product safety rules are defined and enforced in the EU

commitments undertaken go beyond what the current EU framework legislation requires online marketplaces to do, including that on product safety.
The Pledge provides for the following voluntary commitments: (i) cooperation with the Member States' authorities by providing a single point of contact for the notification from such authorities on dangerous products, and by responding to data requests to identify the supply chain of dangerous; (ii) implementation of notice and take-down procedure for dangerous products, including a clear way for customers to notify dangerous product listings; (iii) provision to sellers of information on compliance with EU product safety legislation, requiring sellers to comply with the law, and providing sellers with the link to the list of EU product safety legislation; (iv) implementation of measures aimed at proactively removing banned product groups, preventing the reappearance of dangerous product listings already removed and acting against repeat offenders offering dangerous products. The signatory online intermediaries will also have to report the European Commission the actions taken to implement the above voluntary commitment every six months. So far, two progress reports were published.

9. Other Forms of Liability: Contractual liability

Legislative framework: P2C

Directive 2005/29/EC concerning unfair business-to-consumer commercial practices. [427] Directive 2005/29/EC contrasts unfair business-to-consumer commercial practices, to protect consumers during all the stages of commercial transactions all over Europe. According to the Directive, unfair commercial practices (UCP) are actions or omissions regarding the promotion, sale or supply of a product by a trader to consumers that do not comply with the requirement of professional diligence (the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers corresponding to honest market practice and/or the general principle of good faith in the trader's field of activity), and are likely to materially distort the consumer's economic behaviour.
In particular, the directive identifies two types of unfair practices:

- *misleading commercial practices*: those carrying false information or those that, despite correct, are likely to deceive the average consumer and cause her to take a transactional decision that she would have not otherwise taken, as well as missing, unclear, unintelligible, ambiguous or ultimately misleading information;
- *aggressive commercial practices*: those significantly impairing, by means of harassment, coercion or undue influence, the average consumer's freedom of choice and causing her to take a transactional decision that she would have not otherwise taken.

Annex I of the Directive provides a list of practices that are deemed unfair under all circumstances. Specific rules are set for particularly vulnerable consumers.

Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services.
The directive 2019/770 [428] sets forth rules concerning contracts for the supply of digital content or digital services, with a specific focus on those concerning the conformity of content or service provided with the contract, and on the remedies available in case of non-conformity or non-performance on the side of the trader.
The directive applies to any contract where a trader supplies digital content or digital services to the consumer and the consumer pays or undertakes to pay a price, including those cases where the consumer does not pay a price but provides or undertakes to provide personal data to the trader, unless the personal data provided are only processed for the purpose of supplying the digital content or digital service or for the trader to comply with legal requirements.
Digital content is defined as to include computer programs and mobile applications, as well as video and audio files having digital form, while digital services is described as including services such as cloud computing and social media.
However, the Directive expressly excludes from its scope of application those contract relating to goods with digital elements (regulated by Directive (EU) 2019/771), internet access, texting (such as SMS) – with the exception of number-independent interpersonal communications–, healthcare, gambling services, financial services, software offered under a free and open-source licence – where no price is paid and the personal data provided by the consumer is used only to improve the specific software–, digital content as part of a performance or event, such as digital cinematographic projection, and digital content provided by public sector bodies in accordance with Directive 2003/98/EC.
Pursuant to Article 6-8, the digital content or digital services falling within the scope of application of the Directive must:

- be of the description, quantity and quality, and have other features such as functionality, compatibility, interoperability, as required by the contract;
- be fit for the purpose agreed as part of the contract process;
- be supplied with all accessories, instructions and assistance as required by the contract;
- be updated as stipulated by the contract;

[427] See Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance) PE/83/2019/REV/1, OJ L 328, 18.12.2019, p. 7–28.

[428] See Directive (EU) 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 (Text with EEA relevance.) PE/26/2019/REV/1 OJ L 136, 22.5.2019, p. 1–27.

- be fit for the purposes for which digital content or digital services of the same type would normally be used;
- have the quality and performance features (including functionality, compatibility, accessibility, continuity and security), which the consumer could reasonably expect;
- be supplied with any accessories and instructions which the consumer may reasonably expect to receive;
- comply with any trial or preview version made available before the contract was concluded.

Traders must ensure that the consumer is informed of and supplied with updates, including security updates, necessary to keep the digital content or digital service in conformity. The Directive also contains more detailed rules on the obligation to provide updates.

The trader is held liable in case of any failure to supply the digital content or service, or in case of any lack of conformity existing at the time of the supply and becoming apparent within at least 2 years therefrom; however, if the lack of conformity becomes apparent within 1 year, the consumer is not required to prove its existence at the time of the supply. Likewise, if the digital content or digital service is supplied continuously, liability is set for any lack of conformity occurring and becoming apparent during the supply-period.

As far as remedies are concerned, the Directive prescribes that, in case of failure to supply the digital content or digital service, following a reminder, the consumer may terminate the contract, whereas in case of lack of conformity, the consumer has the right to have the digital content or service brought into conformity, unless it is impossible or would impose disproportionate costs on the trade. If the trader fails to do so, then the consumer is entitled to a proportionate price-reduction, or to terminate the contract. In case of termination of the contract, the consumer is entitled to have full reimbursement from the trader, except for periods when the continuously supplied digital content or digital service was in conformity.

Once the contract is terminated, the traders must comply with the obligations set out by the GDPR and, under certain conditions, they must:

- refrain from using the content – different from personal data – that was provided or created by the consumer when using the digital content or service;
- allow consumers to retrieve such content free of charge, without hindrance from the trader, within a reasonable time.
- from their part, consumers must refrain from using the digital content or service after the contract has been terminated and shall not making it available to third parties.

Directive (EU) 2019/771on certain aspects concerning contracts for the sale of goods [429]. The Directive lays down certain common rules on sales contracts between sellers and consumers for the supply of goods, covering good's conformity with the contract, commercial warranties, and the remedies available to consumer in case of lack of conformity.

Sellers must ensure goods delivered to the consumer conform with the sales contract by:

- complying with what was contractually agreed, e.g. fit the description, type, quantity, quality and possessing the features required by the contract, being fit for the agreed purposes etc.;
- complying with objective conformity criteria, i.e. be fit for the purposes for which similar goods are normally used, correspond to the sample or model shown to the consumer be delivered with the accessories, instructions and packaging that the consumer can reasonably expect and possess the qualities and features that the consumer may reasonably expect.

Sellers are liable for any lack of conformity which becomes apparent within 2 years of delivery. During the first year, the consumer does not have to prove that the defect existed at the time of delivery.

For goods with digital elements, sellers must inform and supply the consumer with all updates needed to keep them in conformity for the duration that the consumer may reasonably expect, unless the digital element of the goods is supplied continuously, in which case updates should be provided throughout the period of supply. Sellers are liable for any lack of conformity which becomes apparent within 2 years of delivery, unless the digital element is to be supplied continuously for a longer period, in which case the seller is liable throughout the period of supply.

If goods are defective ('lack of conformity'), consumers are entitled to a choice between repair and replacement of the goods, free of charge, within a reasonable time and without any major inconvenience. The seller can give an alternative remedy, if the one chosen is impossible or involves disproportionate costs for the seller, a proportionate reduction in price, or termination of the contract, except if the defect is only minor.

Commercial guarantees are binding on the guarantor under the conditions laid down in the guarantee statement and associated advertising, whichever is more advantageous to the consumer. They must be provided to the consumer in plain, intelligible language and in a way that it is accessible for future reference, and must include:

- confirmation the consumer is entitled by law to remedies from the seller for any defects free of charge;
- name and address of the guarantor'
- the procedure for implementing, and the terms of, the guarantee.

Legislative framework: P2B

[429] See Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.) PE/27/2019/REV/1, OJ L 136, 22.5.2019, p. 28–50.

Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services.[430] The Regulation aims to ensure that business users are treated in a fair and transparent way by online platforms, and that they have effective tools for redress when issues occur, with the ultimate aim of enabling a positive regulatory environment for the development of online platforms within the EU.

In particular, the Regulation introduces new rules for online intermediation services – defined as information society services that 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; they are provided to business users on the basis of contractual relationships between the provider of those services and business users offering goods or services to consumers – and for online search engines – defined as digital service allowing users to input queries in order to perform searches of websites 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 –, both aiming to put in contact businesses or professional websites, respectively, and consumers. Importantly, the Regulation applies to providers of those services regardless of whether they are established within or outside the EU, provided that: (i) the business users or corporate website users are established in the Union, and (ii) offer goods and services to consumers located in the Union at least for part of the transaction.

Pursuant to the new rules, online intermediation services must:

- ensure that their terms and conditions are easy to understand and easily available (Article 3);
- clearly state the possible grounds for restricting, suspending or terminating their services, in whole or in part, and, in case of such cases, provide the users with a detailed statement of reasons on a durable medium, with a minimum of 30-day-notice when the decision affects the provision of the service as a whole (Article 3-4);
- give a minim 15 days-notice when modifying their terms and conditions (unless adopted because of specific legal obligations, or to address unforeseen and imminent cybersecurity risks), otherwise said modifications are null and void, and grant the users the right to terminate the contract (Article 3)'
- act in good faith by refraining from retro-active changes to terms and conditions, granting their users' termination and information on whether, after the termination, they may maintain any access to their data (Article 8);
- explain whether they reserve any rights concerning the user's intellectual property, or the platform's ability to market users' goods and services outside the platform itself (Article 3);
- ensure the visibility of the users' identity (Article 3).

Furthermore, the online intermediation services provider' terms and conditions must include:

- the main parameters determining ranking and their relative importance, as well as information about the possibility to influence ranking against direct or indirect remuneration; the same obligation also applies to search engines (Article 5);
- if applicable, a description of any ancillary goods or services that the platform may itself offer to a complement those provided by professional users (Article 6);
- a description of any differentiated treatment given to goods and services offered by the platform themselves or by users under their control (e.g. vertically integrated users); the same obligation also applies to search engines (Article 7);
- information about the technical and contractual possibility of professional users' access to data – be it personal or otherwise – that business users or consumers provide to online intermediation services or that are generated through the use of those services (Article 9);
- if applicable, the legal, economic or commercial consideration for any restriction of the ability of professional users to offer their goods or services under different terms through other channels (Article 10);
- information about the access and functioning of online platforms' internal complaint-handling system, and of the mediators to available for resolving disputes between business users' and the provider (Article 11).

In particular, as far as complaints, mediation, redress and enforcement are concerned, the regulation states that, if employing more than 50 persons or achieving more than €10 million in annual turnover, online intermediation services shall operate an internal system for handling complaints from professional users about non-compliance with a legal obligation laid down in the regulation, or any technological issues, measures taken or behaviour by providers that could affect business users. Complaints must be processed swiftly and effectively, and the outcome communicated individually, in plain and intelligible language (Article 11).

Online intermediation services must publish statistics on the effectiveness of their internal complaint-handling systems and inform oversight bodies including the Observatory on the Online Platform Economy (art 16).

Representative organisations and public bodies have a self-standing right to take action before national courts and to counter any non-compliance with the regulation by providers of online intermediation services and search engines (Article 14).

The adoption of codes of conducts is encouraged (Article 17).

Regulation (EU) 2017/1128 on portability of online content services throughout the EU.[431] Within the EU's digital market strategy, and following the adoption of the EU's roaming rules, this regulation requires online content service providers –

[430] See Regulation (EU) 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 L 186, 11.7.2019, pp. 57-79).

[431] See Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market (OJ L 168, 30.6.2017, pp. 1-11).

video on demand and/or music streaming – to enable subscribers who are temporary staying in another Member States to access their service as they would normally do in their country of residence. In particular, they should be allowed access to the same content, on the same range and number of devices, for the same number of users, with the same functionality, and with no extra charges.
Although no general 'similar quality obligation' is set, providers must not deliberately reduce the quality of their service, and appropriate information shall be given to subscribers. Any service provided in another EU country will be treated as if occurring solely in the subscriber's home EU country.
At the conclusion of a contract and on its renewal, the provider must verify reasonably and effectively the subscriber's country of residence, using no more than two of the sources of information identified by the regulation (e.g. ID card, payment details, etc.), and is not required to make their service available in another EU country if the subscriber fails to present such information. Rights holders can authorise the use of their content without verification of an EU country of residence and can withdraw this authorisation by giving reasonable notice to the provider. The contract between the rights holder and the provider must not restrict this right of withdrawal. Any contractual rule, between the subscriber, provider or rights holders, contrary to this regulation is not enforceable.
Where a free service is provided, the provider may allow access and use to subscribers who are temporarily present in an EU country if their EU country of residence is verified in accordance with the regulation.

10. Other Forms of Liability: Data Protection

Legislative framework

Regulation (EU) 2016/679 (General Data Protection Regulation/GDPR).[432] The GDPR strengthens existing rights, provides for new rights and gives citizens more control over their personal data. These include:

- easier access to their data — including providing more information on how that data is processed and ensuring that that information is available in a clear and understandable way;
- a new right to data portability — making it easier to transmit personal data between service providers;
- a clearer right to erasure ('right to be forgotten') — when an individual no longer wants their data processed and there is no legitimate reason to keep it, the data will be deleted;
- right to know when their personal data has been hacked — companies and organisations will have to inform individuals promptly of serious data breaches. They will also have to notify the relevant data protection supervisory authority.

The GDPR is designed to create business opportunities and stimulate innovation through a number of steps including:

- a single set of EU-wide rules — a single EU-wide law for data protection is estimated to make savings of €2.3 billion per year;
- a data protection officer, responsible for data protection, will be designated by public authorities and by businesses which process data on a large scale;
- one-stop-shop — businesses only have to deal with one single supervisory authority (in the EU country in which they are mainly based);
- companies based outside the EU must apply the same rules when offering services or goods, or monitoring behaviour of individuals within the EU;
- innovation-friendly rules — a guarantee that data protection safeguards are built into products and services from the earliest stage of development (data protection by design and by default);
- privacy-friendly techniques such as pseudonymisation (when identifying fields within a data record are replaced by one or more artificial identifiers) and encryption (when data is coded in such a way that only authorised parties can read it);
- removal of notifications — the new data protection rules will scrap most notification obligations and the costs associated with these. One of the aims of the data protection regulation is to remove obstacles to free flow of personal data within the EU. This will make it easier for businesses to expand;
- impact assessments — businesses will have to carry out impact assessments when data processing may result in a high risk for the rights and freedoms of individuals;
- record-keeping — SMEs are not required to keep records of processing activities, unless the processing is regular or likely to result in a risk to the rights and freedoms of the person whose data is being processed.

[432] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

Directive 2002/58/EC (ePrivacy Directive)[433] and Proposal for a Regulation[434]. Information is exchanged through public electronic communication services such as the internet and mobile and landline telephony and via their accompanying networks.

These services and networks require specific rules and safeguards to ensure the users' right to privacy and confidentiality, as set forth under the ePrivacy Directive.

The ePrivacy Directive sets forth rules to ensure security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications. It also bans unsolicited communications where the user has not given their consent.

Providers of electronic communication services must secure their services by at least:

- ensuring personal data are accessed by authorised persons only;
- protecting personal data from being destroyed, lost or accidentally altered and from other unlawful or unauthorised forms of processing;
- ensuring the implementation of a security policy on the processing of personal data.

The service provider must inform the national authority of any personal data breach within 24 hours. If the personal data or privacy of a user is likely to be harmed, they must also be informed unless specifically identified technological measures have been taken to protect the data.

EU countries must ensure the confidentiality of communications made over public networks. In particular they must:

- prohibit the listening, tapping, storage or any type of surveillance or interception of communications and traffic data without the consent of users, except if the person is legally authorised and in compliance with specific requirements;
- guarantee that the storing of information or the access to information stored on user's personal equipment is only permitted if the user has been clearly and fully informed, among other things, of the purpose and been given the right of refusal.

When traffic data are no longer required for communication or billing, they must be erased or made anonymous. However, service providers may process these data for marketing purposes for as long as the users concerned give their consent. This consent may be withdrawn at any time.

User consent is also required in a number of other situations, including:

- before unsolicited communications (spam) can be sent to them. This also applies to short message services (SMSs) and other electronic messaging systems;
- before information (cookies) is stored on their computers or devices or before access to that information is obtained - the user must be given clear and full information, among other things, on the purpose of the storage or access;
- before telephone numbers, e-mail addresses or postal addresses can appear in public directories.

EU countries are required to have a system of penalties including legal sanctions for infringements of the directive.

The scope of the rights and obligations can only be restricted by national legislative measures when such restrictions are necessary and proportionate to safeguard specific public interests, such as to allow criminal investigations or to safeguard national security, defence or public security.

The ePrivacy Regulation imposes the following obligations on electronic communications networks and services:

- Metadata (i.e. 'data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication') shall require the consent of the end user to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous'.
- Content (i.e. – 'the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound') can be processed only 'for the sole purpose of the provision of a specific service to an end-user, if the end user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content' or 'if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority'.
- End users given shall be given 'the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues'.
- 'Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the

[433] See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

[434] See European Commission (2017). Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM(2017) 10 final Brussels, European Commission.

terminal equipment of an end user or processing information already stored on that equipment. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting'. In this respect, Recital 23 clarifies that browsers practice of having a default 'accept all cookies' setting should be changed and thus 'end-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies')'.

- The obligation to respect the confidentiality of the communications;

The end users have a right to compensation for damages suffered against the electronic communications networks and services that they caused by infringing the Regulation a material or non-material damage to the ends users, 'unless the infringer proves that it is not in any way responsible for the event giving rise to the damage in accordance with Article 82 of Regulation (EU) 2016/679'. End users are also entitled to the remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679.

OA-03-20-811-EN-N

Given the central role that online platforms (OPs) play in the digital economy, questions arise about their responsibility in relation to illegal/harmful content or products hosted in the frame of their operation.

Against this background, this study reviews the main legal/regulatory challenges associated with OP operations and analyses the incentives for OPs, their users and third parties to detect and remove illegal/harmful and dangerous material, content and/or products. To create a functional classification which can be used for regulatory purposes, it discusses the notion of OPs and attempts to categorise them under multiple criteria. The study then maps and critically assesses the whole range of OP liabilities, taking hard and soft law, self-regulation and national legislation into consideration, whenever relevant.

Finally, the study puts forward policy options for an efficient EU liability regime: (i) maintaining the status quo; (ii) awareness-raising and media literacy; (iii) promoting self-regulation; (iv) establishing co-regulation mechanisms and tools; (v) adopting statutory legislation; (vi) modifying OPs' secondary liability by employing two different models – (a) by clarifying the conditions for liability exemptions provided by the e-Commerce Directive or (b) by establishing a harmonised regime of liability.

This is a publication of the Scientific Foresight Unit (STOA)
EPRS | European Parliamentary Research Service

ISBN 978-92-846-7499-2|doi:10.2861/619924|QA-03-20-811-EN-N