EUROPEAN
COMMISSION

Brussels, 15.12.2020
SWD(2020) 348 final

PART 1/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

{COM(2020) 825 final} - {SEC(2020) 432 final} - {SWD(2020) 349 final}

Table of contents

Glossary

Term or acronym	*Meaning or definition*
Collaborative economy platform	an online platform ensuring an open marketplace for the temporary usage of goods or services often provided by private individuals. Examples include temporary accommodation platforms, ride-hailing or ride-sharing services.
Competent authorities	the competent authorities designated by the Member States in accordance with their national law to carry out tasks which include tackling illegal content online, including law enforcement authorities and administrative authorities charged with enforcing law, irrespective of the nature or specific subject matter of that law, applicable in certain particular fields.
Content provider	a user who has submitted information that is, or that has been, stored at his or her request by a hosting service provider.
CSAM	Child Sexual Abuse Material, for the purposes of this IA refers to any material defined as 'child pornography' and 'pornographic performance' in Directive 2011/93/EU
Digital service	used here as synonym to an information society service – see definition below
Erroneous removal	the removal of content, goods or services offered online where such removal was not justified by the illegal nature of the content, goods, or services, or the terms and conditions of the online service, or any other reason justifying the removal of content, goods or services.
FTE	Full time equivalent
Harmful behaviours/activities online	while some behaviours are prohibited by the law at EU or national level (see definitions for illegal content and illegal goods), other behaviours could potentially result in diverse types of harms, without being illegal as such. A case in point are coordinated disinformation campaigns which may lead to societal impact or individual harm under certain conditions. Some content can also be particularly damaging for vulnerable categories of users, such as children, but not for the general public. Such notions remain, to a certain extent, subjective.
Hosting service provider	a provider of information society services consisting of the storage of information provided by the recipient of the service at her request, examples include social media platforms, video streaming services, video, image and audio sharing services, file sharing and other cloud services
Illegal content	any information which is not in compliance with Union law or the law of a Member State concerned;
Illegal activity	any activity which is not in compliance with Union law or the law

	of a Member State concerned;
Illegal goods or services	refer to the illegal sale of goods or services, as defined in EU or national law. Examples include the sale of counterfeit or pirated goods, of dangerous or non-compliant products (i.e. food or non-food products which do not comply with the health, safety, environmental and other requirements laid down in European or national law), of products which are illegally marketed, of endangered species.
Illegal hate speech	The following serious manifestations of racism and xenophobia that must constitute an offence in all EU countries: (a) public incitement to violence or hatred in respect of a group of persons or a member of such a group defined by reference to colour, race, religion or national or ethnic origin; (b) public condoning, for a racist or xenophobic purpose, of crimes against humanity and human rights violations; (c) public denial of the crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 April 1945 insofar as it includes behaviour which is contemptuous of, or degrading to, a group of persons defined by reference to colour, race, religion or national or ethnic origin; (d) public dissemination or distribution of tracts, pictures or other material containing expressions of racism and xenophobia; (e) participation in the activities of groups, organizations or associations, which involve discrimination, violence, or racial, ethnic or religious hatred.
Information Society Service	a service 'normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services', as defined in Directive (EU) 2015/1535. The definition covers a very large category of services, from simple websites, to online intermediaries such as online platforms, or internet access providers.
Very large online platforms	online platforms with a significant societal and economic impact by covering, among their monthly users, at least 10% of the EU population (approximately 45 million users).
Law enforcement authorities	the competent authorities designated by the Member States in accordance with their national law to carry out law enforcement tasks for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including in connection to illegal content online;
Notice	any communication to a hosting service provider that gives the latter knowledge of a particular item of illegal content that it transmits or stores and therefore creates an obligation for it to act expeditiously by removing the illegal content or disabling/blocking access to it. Such an obligation only arises if the notice provides the internet hosting service provider with actual awareness or knowledge of illegal content.

Online platforms	a variety of 'hosting service providers' such as social networks, content-sharing platforms, app stores, online marketplaces, ride-hailing services, online travel and accommodation platforms. Such services are generally characterised by their intermediation role between different sides of the market – such as sellers and buyers, accommodation service providers, or content providers – and oftentimes intermediate access of user-generated content.
Online intermediary service	digital service that consist of transmitting or storing content that has been provided by a third party, the E-commerce Directive distinguishes three types of intermediary services: mere conduit (transmitting of data by an internet access provider), caching (i.e. automatically making temporary copies of web data to speed up technical processes) and hosting
Recommender systems	refer to the algorithmic systems used by online platforms to give prominence to content or offers, facilitating their discovery by the users. Recommender systems follow a variety of criteria and designs, sometimes personalised for the users, based on their navigation history, profiles, etc., other times based purely on the content analogy or ratings.
Trusted flagger/third party	an individual or entity which is considered by a hosting service provider to have particular expertise and responsibilities for the purposes of tackling illegal content online;
Users	Refers, throughout the report, to any natural or legal person who is the recipient of a digital service

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

1 The President of the Commission announced as one of her political priorities[1] a new Digital Services Act as a key measure in her agenda for shaping Europe's digital future[2], to establish a fair and competitive digital economy and to build an open, democratic and sustainable society. The Digital Services Act together with the Digital Markets Act are intended as a comprehensive package of measures for the provision of digital services in the European Union and seek to address in particular the challenges posed by online platforms.

2 In the Digital Services Act, which is underpinned by this impact assessment report, the intervention focuses on deepening the single market for digital services and establishing clear responsibilities for online platforms as well as other intermediary services to protect their users from the risks they pose, such as illegal activities online and risk to their fundamental rights. The Digital Markets Act complements these provisions and focuses on the gatekeeper role and unfair practices by a prominent category of online platforms.

3 Digital services have become an important backbone of the digital economy and have deeply contributed to societal transformations in the EU and across the world. At the same time, they also raise significant new challenges. It is for this reason that updating the regulatory framework for digital services has become a priority, not only in the European Union, but also around the globe.

4 In the Communication 'Shaping Europe's Digital Future'[3], the Commission made a commitment to update the horizontal rules that define the responsibilities and obligations of providers of digital services, and online platforms in particular.

5 Both the European Parliament and the Council of the European Union share the sense of urgency to establish at EU level a renewed and visionary framework for digital services. The European Parliament proposed three own initiative reports, focusing on specific aspects in the provision of digital services: considerations for the single market, responsibilities for online platforms for tackling illegal content, and protection of fundamental rights online.[4] The Council's Conclusions[5] welcomed the Commission's announcement of a Digital Services Act, emphasised *'the need for clear and harmonised evidence-based rules on responsibilities and accountability for digital services that would guarantee internet intermediaries an appropriate level of legal certainty*', and stressed *'the need to enhance European capabilities and the cooperation of national authorities, preserving and reinforcing the fundamental principles of the Single Market and the need to enhance citizens' safety and to protect their rights in the digital sphere across the Single Market'*. The call was reiterated in the Council's Conclusions of 2nd October 2020[6].

6 Not only governments and legislators have expressed the need to respond to the changes in the digital landscape. The nearly 3000 contributions received in response to the most

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf
[2] https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf
[3] https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf
[4] Annex 13 presents a brief summary of the reports and a map of how the impact assessment explores the points raised in the reports
[5] Council Conclusions on Shaping Europe's Digital Future, 8711/20 of 9 June 2020, https://www.consilium.europa.eu/media/44389/st08711-en20.pdf
[6] https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf

recent open public consultation concerning this initiative highlight the significant public interest to re-imagine how digital services influence our daily lives.

7 The challenge of addressing the changed and increasingly complex ecosystem of digital services is not only an EU endeavour, but also prominent at international level. It is discussed at the UN, Council of Europe, OSCE, WTO, and OECD and it is regularly on the agenda of G7/G20 meetings. It is also high on the agenda of many third country jurisdictions across the world.

8 The EU has a wide range of trade commitments in sectors covering digital services. This initiative will be in full compliance with the EU's international obligations, notably in the multilateral agreements in the World Trade Organisation and in its regional trade agreements.

9 Besides the Treaty provisions, the basic framework regulating the provision of digital services in the internal market is defined in the E-Commerce Directive dating from 2000. The goal of that directive is to allow borderless access to digital services across the EU and to harmonise the core aspects for such services, including information requirements and online advertising rules, as well as setting the framework for the liability regime of intermediary services – categorised as 'mere conduits', 'caching services', and 'hosting services' – for third party content.

10 Since then, the nature, scale, and importance of digital services for the economy and society has dramatically changed. Business models, which emerged with large online platforms such as social networks or marketplaces, have changed the landscape of digital services in the EU. These services are now used by a majority of EU citizens on a daily basis, and are based on multi-sided business models underpinned by strong network effects.

11 In response to the evolving digital landscape, several service-specific and sector-specific legal acts several have complemented the E-Commerce Directive by regulating different issues concerning the provision of digital services, such as revised data protection rules, copyright rules and rules concerning audiovisual services or consumer *acquis*.

12 The Court of Justice of the EU has contributed to the uniform interpretation and application of the E-Commerce Directive, by interpreting and reaffirming its core principles in the context of new digital services and technologies.

13 More recently, the Commission has also taken a series of targeted measures, both legislative[7] and self-regulatory[8], as well as coordinated enforcement actions in the

[7] Legislation addressing specific types of illegal goods and illegal content includes: the market surveillance regulation, the revised audio-visual media services directive, the directive on the enforcement of intellectual property rights, the directive on copyright in the digital single market, the regulation on market surveillance and compliance of products, the proposed regulation on preventing the dissemination of terrorist content online, the directive on combatting the sexual abuse and sexual exploitation of children and child pornography, the regulation on the marketing and use of explosives precursors etc. The Directive on better enforcement and modernisation of EU consumer protection rules added transparency requirements for online marketplaces vis-à-vis consumers which should become applicable in May 2022.

[8] e.g. the EU Internet Forum against terrorist propaganda online, the Code of Conduct on countering illegal hate speech online, the Alliance to better protect minors online under the European Strategy for a better internet for children and the WePROTECT global alliance to end child sexual exploitation online, the Joint Action of the consumer protection cooperation network authorities, Memorandum of understanding against counterfeit goods, the Online Advertising and IPR Memorandum of Understanding, the Safety Pledge to improve the safety of products sold online etc. In the framework of

framework of the Consumer Protection Cooperation Regulation (CPC)[9], for addressing the spread of certain types of illegal activities online such as copyright-protected content, practices infringing EU consumer law, dangerous goods, illegal hate speech, terrorist content, or child sexual abuse material. These targeted measures do not address, however, the systemic risks posed by the provision and the use of digital services, nor the re-fragmentation of the single market and the competition imbalances brought about by the emergence of very large digital service providers on a global scale.

14 This impact assessment explores the changed nature, scale and influence of digital services, in particular online platforms. The assessment tracks key drivers which have led to societal and economic challenges posed by the digital services ecosystem and outlines the options to address them and improve the functioning of the digital single market. This Impact Assessment builds on the evaluation[10] of the E-Commerce Directive[11], annexed to the report.

2. PROBLEM DEFINITION

2.1. Context and scope

15 Digital services[12] have been defined as 'services normally provided against remuneration, at a distance, by electronic means and at the individual request of a recipient of services'. This definition covers in principle a wide-scope of very diverse services, including:

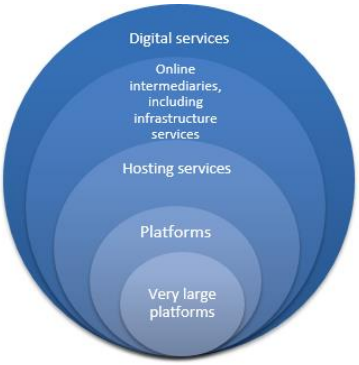


Figure 1 Types of digital services

- apps, online shops, e-games, online versions of traditional media (newspapers, music stores), Internet-of-Things applications, some smart cities' services, online encyclopaedias, payment services, online travel agents, etc., but also
- services provided by 'online intermediaries', ranging from the very backbone of the internet infrastructure, with internet service providers, cloud infrastructure services, content distribution networks, to messaging services, online forums, online platforms (such as app stores, e-commerce marketplaces, video-sharing and media-sharing platforms, social networks, collaborative economy platforms etc.) or ads intermediaries.

---

the Consumer Protection Cooperation Regulation (CPC), the consumer protection authorities have also taken several coordinated actions to ensure that various platforms (e.g. travel booking operators, social media, online gaming platforms, web shops) conform with consumer protection law in the EU. A package of measures was also adopted to secure free and fair elections - https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681

[9] In the framework of the Consumer Protection Cooperation Regulation (CPC), the consumer protection authorities have also taken several coordinated actions to ensure that various platforms (e.g. travel booking operators, social media, online gaming platforms, and webshops) conform with consumer protection law in the EU https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/coordinated-actions_en.

[10] See Annex 5 for details about the evaluation of the E-Commerce Directive.

[11] 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

[12] The term "Digital Service" as used in this document is synonymous with term 'information society services', as defined in the E-Commerce Directive and the Transparency Directive 2015/1535.

16 All of these services have evolved considerably over the past 20 years as many new ones have appeared. The landscape of digital services continues to develop and change rapidly along with technological transformations and the increasing availability of innovations[13].

17 For **e-commerce** alone (for services and goods sold online), the increase has been steady over the past 20 years. Today around 20% of European businesses are involved in e-commerce. Out of those who sell goods online, 40% are using online marketplaces to reach their customers.[14] Whereas in 2002, shortly after the entry into force of the E-Commerce Directive, only 9% of Europeans were buying goods online, over 70% shop online today.[15]

18 A study conducted for the European Parliament[16] emphasises the strategic importance of e-commerce and digital services in boosting the opportunities for **SMEs to access new markets** and new consumer segments, accelerating their growth, affording **lower prices for consumers** (2% to 10% advantage compared to offline sales), and enhancing **territorial cohesion** in the Union, blurring geographic dependencies between markets. The study estimates overall welfare gains from e-commerce to be between 0.3 and 1.7% of EU-27 GDP.

19 While some **online platforms** did exist at the end of the 1990s, their scale, reach and business models were in no way comparable to their current influence in the market and the functioning of our societies. In 2018, 76% of Europeans said[17] that they were regular users of video-sharing or music streaming platforms, 72% shopped online and 70% used social networks. Through the advent of online platforms, many more economic activities were open to online consumption, such as transport services and short-term accommodation rental, but also media production and consumption and important innovations were brought by user-generated content.

20 **Online advertising services** are an area of particular evolution over the past 20 years: whereas online commercial communications started with simple email distribution lists, they are now an enormous industry[18], with several types of intermediaries involved in the placement of ads.

21 The evolution is not limited to consumer-facing digital services, far from it. In particular, in what concerns online intermediaries **providing the technical infrastructure** of the internet, technological developments and improvement of capabilities have been staggering. The core internet infrastructure set by internet access services and DNS operators is now also supported by other types of technical services such as content delivery networks (CDN), or cloud infrastructure services. They are all fundamental for any other web application to exist and their actions have a major impact on the core access to internet services and information. The resilience, stability and security of core

[13] From optimisations through network technologies to development of artificial intelligence applications or blockchain technology and distributed data processing.

[14] 40% in 2019 in EU27, according to ESTAT https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do See also (Eurobatometer - TNS, 2016) for more granular data based on a 2016 survey

[15] (Duch-Brown & Martens, 2015)

[16] (Iacob & Simonelli, 2020)

[17] (Eurobarometer - TNS, 2018)

[18] In the first half of 2019 online advertising pending in Europe amounted to 28.9 billion Euros. The growth rate of online advertising in the same period was around 12.3% (https://www.statista.com/topics/3983/digital-advertising-in-europe/).

services such as DNS are a precondition for digital services to be effectively delivered to and accessed by internet users.

22 While online platforms present particular opportunities and concerns and are most prominently referred to, all these intermediary services have a strategic importance for the development of virtually all sectors in the European economy and, increasingly so, in social interactions and societal transformations. There are several key observations to note:

23 *First*, digital services are **inherently cross-border services.** The ability to provide and access any digital service from anywhere in the Union is increasingly a feature citizens expect, while also expecting to be well protected from illegal content and activities. This **raises the stakes when barriers arise for the provision of digital services,** in particular to maintain a rich, diverse, and competitive landscape of digital services that can thrive in the EU.

24 *Second*, online intermediary services are **vital for the backbone of the internet** (e.g. internet access services, cloud infrastructure, DNS) and **agile innovators** and first users of new technologies (from internet of things, to artificial intelligence). They are a strategic sector for the European economy, and a core engine for the digital transformation.

25 *Third*, the **particular business model of online platforms** has emerged over the last two decades, connecting users with suppliers of goods, content or services. These online platforms are often characterised as multi-sided markets, benefiting from very strong network effects. The value of the platform service increases rapidly as the number of users increase.

26 *Fourth, w*hile such platforms are traditionally major innovators in terms of services and products, they now have become the source of new **risks and challenges for their users** and society at large.

27 *Fifth*, while there are approximately 10.000[19] micro, small or medium size online platforms, millions of users concentrate around a small number of very large online platforms, be it in e-commerce, social networks, video-sharing platforms etc. This transforms such **very large platforms into *de facto* public spaces for businesses to find consumers, for authorities, civil society or politicians to connect with citizens and for individuals to receive and impart information**.

28 Such large platforms have come to play a particularly important role in our society and our economy, different in scale and scope from that of other similar services with lower reach. The way they organise their services has a significant impact, e.g. on the offer of illegal goods and content online, as well as in defining 'choice architecture' that determines the options that users have in accessing goods, content, or services online.

29 *Finally*, societal trends related to how we use technology, work, learn or shop are changing rapidly. While these trends were already unfolding before the COVID-19 outbreak, we are seeing an acceleration of the digitalization trend, which is likely to lead to a 'new normal' after the COVID-19 crisis and an even more important role for digital services in our daily lives in the future. Online sales of basic goods alone have grown by 50% on average in Europe[20] since the offset of the pandemics. At the same time, the

[19] Dealroom database, see *infra*, p *24*

[20] https://www.oecd.org/coronavirus/policy-responses/connecting-businesses-and-consumers-during-covid-19-trade-in-parcels-d18de131/#figure-d1e204

crisis has exposed the weaknesses of our reliance on digitalization, as we have seen an important growth in platform-enabled crime, such as COVID-19-related scams and exchange of child sexual abuse material[21].

30 Against this background, the Impact Assessment covers all types of online intermediaries, with a particular focus on online platforms and the risks and harms they may represent, and the challenges they are facing in the Single Market.

2.2. What are the problems?

31 This Impact Assessment analyses the three core issues related to the **governance of digital services in the European single market**, as follows:

Table 1 Summary of main problems and scope

Main problems	***For whom is this a problem?***	
	Main types of digital services concerned	***Other stakeholders primarily affected***
1. *Serious societal and economic risks and harms of online intermediaries: illegal activities online, insufficient protection of the fundamental rights and other emerging risks*	Illegal activities and risks to fundamental rights: **all types of online intermediaries, with particular impacts where online platforms are concerned** Other emerging risks: **primarily related to online platforms**	Citizens and consumers Businesses prejudiced by illegal activities Law enforcement
2. Ineffective supervision of services & insufficient administrative cooperation, creating hurdles for services and weakening the single market	**Mostly as regards supervision of online platforms,** with particular challenges where platforms cover a large part of the single market	Citizens National authorities
3. *Legal barriers for services: preventing smaller companies from scaling up and creating advantages for large platforms, equipped to bear the costs*	**In particular online platforms as primarily targeted by the legal fragmentation, but also other online intermediaries**	Businesses depending on online intermediaries

32 The Impact Assessment builds on the evaluation of the E-Commerce Directive in Annex 5. This evaluation concludes the following main points.

Box 1: Main conclusions and issues emerging from the Evaluation Report

First, the evaluation concludes that the core principles of the E-Commerce Directive regulating the functioning of the internal market for digital services remain very much valid today. The evaluation shows that the directive enabled growth and accessibility of digital services cross-border in the internal market. This concerns all layers of the internet and the web and has enabled successful entry and growth of many EU companies in different segments of the market.

[21] Europol, *Pandemic profiteering: how criminals exploit the COVID-19 crisis*, March 2020, see: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis.

At the same time, the evaluation points to clear evidence of legal fragmentation and differentiated application of the existing rules by Member States, and ultimately by national courts. There is also an increased tendency of Member States to adopt legislation with extraterritorial effects and enforce it against service providers not established in their territory. Such enforcement in consequence reduces trust between competent authorities and undermines the well-functioning internal market as well as the existing cooperation mechanisms.

In this context, the evaluation also shows that Member States make little use of the cooperation mechanism provided for in the E-Commerce Directive. The evaluation shows that the existing mechanism, whose existence is still considered very relevant and important overall for the functioning of the single market for digital services, requires a more effective set-up to ensure trust between Member States and an effective supervision and sanctioning of digital services posing particular challenges, such as online platforms.

Second, the evaluation concludes that the liability regime for online intermediaries continues to establish the key regulatory pillar enabling conditions for the existence and growth of intermediary services as well as for the fair balance in the protection of fundamental rights online. If, in 1996, the Commission signalled that the objective when discussing the liability and responsibilities of intermediaries in respect of stored user content was "to design a legal regime that assists 'host service providers, whose primary business is to provide a service to customers, to steer a path between accusations of censorship and exposure to liability'[22], that objective remains equally valid today.

The evaluation shows that the liability regime for online intermediaries provided for a necessary minimum of legal certainty for online intermediaries as initially pursued. However, conflicting interpretations in national court cases (sometimes even within the same Member State) have introduced a significant level of uncertainty; in addition, an increasing fragmentation of the single market raises barriers for EU scale-ups to emerge. Furthermore, the evaluation also shows that the relevant provisions have only partially achieved the balancing objective of protecting fundamental rights. They provide stronger incentives for the removal of content than to protect legal content and also lack appropriate oversight as well as due process mechanisms especially in situations where the subsequent action is taken by private sector entities, rather than public sector authorities.

In addition, the existing categories defining online intermediaries are somewhat outdated, in particular in light of the evolution of services and underlying technology. Some providers exercise a clear influence over the hosted content, leading the user to confusion as to the identity or origin of the goods or services she or he views – blurring the line of what is expected from an intermediary. Finally, without prejudice to the exemption of liability, the current framework lacks necessary obligations on due diligence as regards third party content to ensure that risks brought by the dissemination of illegal content, goods or services online are appropriately addressed.

Third, the evaluation shows that a series of transparency and consumer-facing provisions[23] included in the Directive are still relevant. The provisions have set the minimum conditions for consumer trust and provision of digital services and have been largely complemented – but not overwritten - by a rich corpus of further rules and

[22] European Commission, Illegal and Harmful Content Communication, COM(96) 487, pp. 12–13.

[23] With a proportionality concern, these aspects are succinctly addressed in the impact assessment report, focused instead on the most poignant issues related to the systemic concerns around digital services.

harmonisation measures in the areas such as consumer protection and conclusion of contracts at a distance, including by online means. This is not to say there are no challenges; several enforcement actions by the Consumer Protection Cooperation (CPC) Network, show that some provisions, such as basic information requirements, suffer from a patchy and diverging application in practice. Furthermore, the fundamental changes in the variety and scale of information society services, as well as of the technologies deployed and online behaviour, have led to the emergence of new challenges, not least in terms of transparency of online advertising and algorithmic decision-making consumers and businesses are subject to.

33 The following sub-sections present in more detail the problems identified and their causes, as well as the expected evolution of the problems.

2.2.1. Serious risks and harms brought by digital services

European citizens are exposed to increasing risks and harms online – from the spread of illegal activities, to infringements of fundamental rights and other societal harms. These issues are widespread across the online ecosystem, but they are most impactful where very large online platforms are concerned, given their wide reach and audiences. Such platforms play today a systemic role in amplifying and shaping information flows online. Their design choices have a strong influence on user safety online, the shaping of public opinion and discourse, as well as on online trade. Such design choices can cause societal concerns, but are generally optimised to benefit the often advertising-driven business models of platforms. In the absence of effective regulation and enforcement, platforms set the rules of the game, without effectively mitigating the risks and the societal and economic harm they cause.

a) **Illegal activities online**

34 The use of digital services and the opportunities these services provide for electronic commerce and information sharing is now present throughout society and the economy. Correspondingly, the misuse of services for illegal activities has also expanded significantly. This includes illegal activities, as defined at both European and at national level, such as:

- the sale of illegal goods, such as dangerous goods, unsafe toys, illegal medicines, counterfeits, scams and other consumer protection infringing practices, or even wildlife trafficking, illegal sale of protected species, etc.;
- the dissemination of illegal content such as child sexual abuse material, terrorist content, illegal hate speech and illegal ads targeting individuals, IPR infringing content, etc.;
- the provision of illegal services such as non-compliant accommodation services on short-term rental platforms, illegal marketing services, services infringing consumer protection provisions, or non-respect for extended producer responsibility obligations.

Scale of the spread of illegal content and activities

35 The **scale of the spread of illegal activities** varies and the data available for accurately measuring these phenomena is scarce. Quantitative indications are generally only available as approximations, usually based on detected crimes. As a result, the actual occurrence of illegal activities online is expected to be higher than the reported indicators as many activities are likely to go unreported. At the same time, in particular large online

platforms regularly release some reports including content removal figures. Even though such removals are usually based on standards of private community rules, covering not only illegal content but also harmful content and other content breaching the terms of service, the reported numbers can give upper bound indications.

Box 2: Scale of illegal activities: some examples

It is estimated that total imports of **counterfeit goods** in Europe amounted to EUR 121 billion in 2016 [24], and 80% of products detected by customs authorities involved small parcels[25], assumed to have been bought online internationally through online market places or sellers' direct websites. Consumers are buying increasingly more from producers based outside of Europe (from 14% in 2014 to 27% in 2019).[26]

For **dangerous products**, the Rapid Alert System for dangerous non-food products (Safety Gate/RAPEX) registers between 1850 and 2250 notifications from Member States per year[27]. In 2019, around 10% were confirmed to be also related to online listings, while the availability of such products online is very likely higher. Consumer organisations reported on investigations in which known non-compliant goods were made available via online market-places without any checks, detection, or hindrance[28]. In this regard, the COVID-19 crisis has also cast a spotlight on the proliferation of illegal goods online, breaching EU safety and protection requirements or even bearing false certificates of conformity[29], especially coming from third countries. The coordinated action of the CPC authorities targeting scams related to COVID-19 obliged online platforms to remove millions of misleading offers aimed at EU consumers[30].

When it comes to categories of illegal content online, for **child sexual abuse material** the US hotline, which processes the largest number of reports, the National Centre for Missing and Exploited Children, has seen a significant growth in reports globally reaching 16.9 million in 2019, which is a doubling from 8.2 million in 2016[31]. This trend is confirmed by the EU network of hotlines, INHOPE, which indicate that images processed between 2017 and 2019 almost doubled[32]. It is important to note that reports have multiple images and that the illegality is subject to verification by the clearing houses, INHOPE statistics, show that upwards of 70% of images reported are illegal.

For **illegal hate speech**, it is particularly difficult to estimate the volumes and spread of content, not least since most of the information available refers to platforms' own definitions of hate speech and not to legal definitions, such as the EU-level reference[33].

[24] (OECD/EUIPO, 2019)

[25] (European Commission, 2019) *apud* (European Commission, 2020)

[26] https://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals#General_overview

[27] https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/pages/rapex/index_en.htm

[28] https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html.

[29] https://www.oecd.org/coronavirus/policy-responses/protecting-online-consumers-during-the-covid-19-crisis-2ce7353c/#section-d1e96

[30] https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/scams-related-covid-19_en

[31] https://web.archive.org/web/20190928174029/https://storage.googleapis.com/pub-tools-public-publication-data/pdf/b6555a1018a750f39028005bfdb9f35eaee4b947.pdf
https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf

[32] https://www.inhope.org/media/pages/the-facts/download-our-whitepapers/803148eb1e-1600720887/2020.09.18_ih_annualreport_digital.pdf

[33] Illegal hate speech, as defined by the Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law and

As an example, Facebook reported[34] to have taken action in April-June 2019 against 4.4 million pieces of content considered hate speech according to the definition of its community standards[35] and, comparatively, 22.5 million in the same period in 2020. Further, even where minimum standards were set for reporting hate speech under the national legislation, such as NetzDG[36] in Germany, individual companies' implementation renders the data non-comparable, where for example Twitter reports nearly 130,000 reports per million users, Facebook only recorded 17 reports per million users which is a clear indication that the numbers do not adequately reflect the scale of the issue[37]

36 To better contextualise the online component of such illegal activities, the Commission ran a Flash Eurobarometer survey[38] among a random sample of over 30,000 internet users in all Member States, testing user perception of the frequency and scale of illegal activities or information online. 60% of respondents thought they had seen at least once some sort of illegal content online. 41% experienced scams, frauds or other illegal commercial practices. 30% thought they had seen hate speech (according to their personal understanding of the term), 27% had seen counterfeited products and 26% has seen pirated content. These categories are consistently the highest in all Member States, with some variations.

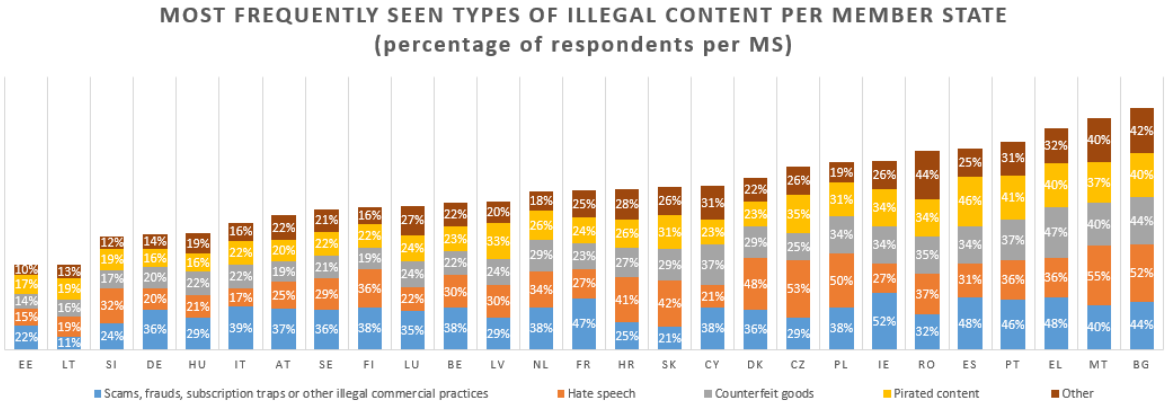


Figure 2: Most frequently seen types of illegal content on online platforms. Flash Eurobarometer on illegal content online, 2018 (N= 32,000 respondents)

Services concerned in the spread of illegal activities are diverse in nature and size

37 There are several ways through which digital services contribute to illegal activities online. *First*, **digital service providers** (e.g. websites of online shops, content apps, gambling services, online games) can infringe the law themselves, frequently by

national laws transposing it, means all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin.

[34] https://transparency.facebook.com/community-standards-enforcement#hate-speech

[35] By contrast with the EU definition, Facebook defines hate speech as 'violent or dehumanizing speech, statements of inferiority, calls for exclusion or segregation based on protected characteristics, or slurs. These characteristics include race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity, and serious disability or disease.' https://transparency.facebook.com/community-standards-enforcement#hate-speech

[36] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Network Enforcement Act)

[37] Wagner, Ben, Krisztina Rozgonyi, Marie-Therese Sekwenz, Jatinder Singh, and Jennifer Cobbe. 2020. "Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act."

[38] (Eurobarometer - TNS, 2018)

misleading and scamming consumers, or by selling illegal products. This remains a persistent problem. This is, to a large extent, an issue of enforcement and almost 80% of all notifications and assistance requests sent by Member States for cross-border issues concern infringements by such online services[39].

38 *Second*, with the increased use of **online platforms**, more opportunities for disseminating and amplifying the dissemination of illegal content, goods or services have emerged. Perpetrators use these services, from hosting content on file sharing services, to disseminating hyperlinks through the most used social network platforms **where the widest audiences can be reached[40]**. Further, such services are themselves built for optimising access to content or commercial offers, respectively, and their systems can be manipulated and abused to drive users more easily towards illegal goods, content or services. This is even more acutely the case where very large online platforms are concerned, where the highest numbers of users can be reached and where the amplification of illegal content and activity is consequently most impactful. These very large online platforms lack the necessary incentives and oversight to guarantee users' safety and privacy and to prevent deceptive and fraudulent practices.

39 Challenges addressing the scale and the spread of illegal goods, services and content are further amplified by the accessibility of services in the Union offered from providers established in third countries, which are currently not bound by the E-Commerce Directive.[41]

Box 3: Examples of misuse of online intermediary services for disseminating illegal content

According to INHOPE[42], 84% of **child sexual abuse material** (CSAM) is shared through image hosting websites, 7% through file hosts, 5% on other websites and 4% through other services, including social networking sites or , forums or banner sites. NCMEC data shows that, while the highest shares of the reported content comes from Facebook and its subsidiaries, including its private messaging services, largely due to the fact that Facebook are taking active steps to find CSAM. It is expected that large numbers of CSAM material is also shared on a variety of other services of different sizes.

For **terrorist content**, the 2018 Impact Assessment accompanying a proposal for a Regulation on Terrorist Content[43] contained some relevant data. Out of some 150 companies to which Europol had sent referrals, almost half offered file hosting and sharing services (mostly micro-enterprises), and the rest were mainstream social media, web hosting services, as well as online media sharing platforms (both big and medium-sized enterprises). Overall, one out of ten companies was a medium or large enterprise, whereas the rest were small and micro enterprises. In terms of the volume of content, 68% of Europol referrals were addressed to micro, small and unregistered companies in 2017.

[39] Report from the IMI system, See also Annex 8

[40] https://rusi.org/sites/default/files/20190628_grntt_paper_2_0.pdf

[41] See in particular recital 58 of the E-Commerce Directive.

[42] https://www.inhope.org/EN https://www.inhope.org/EN

[43] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf (Concerning Proposal COM/2018/640 final)https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf (Concerning Proposal COM/2018/640 final)

b) Emerging systemic societal risks posed by online platforms

40 **Online platforms pose particular risks, different in their nature and scale from other digital services**. With the staggering volumes of information and commercial offers available online, platforms have become important players in the 'attention economy'[44]. Very large platforms now have a systemic role in amplifying and shaping information flows online and for the largest part of EU citizens, businesses and other organisations. This is at **the core of the platform business model**: matching users with, presumably, the most relevant information for them, and optimising the design to maximise the company's profits (through advertising or transactions, depending on the type of platform).

41 At the same time, their design choices have a strong influence on user safety online, the shaping of public opinion and discourse, as well as on online trade. **Illegal content** shared through such platforms can be amplified to reach wide audiences.[45] Particular challenges emerge where content is disseminated at a significant speed and scale across platforms, as it was the case with the terrorist attack in Christchurch[46], with the potential to incite further violence, and with severe damage to the victims and their families.

42 Risks, however, go beyond the spread of illegal activities. Negative effects also stem from the manipulation of platforms' systems to amplify, oftentimes through coordinated attacks and inauthentic behaviours, certain messages or behaviours online. Such practices lead to a deliberate misuse of the platforms' system for instigation to violence or self-harm (harmful in particular to children and in the context of gender-based online violence), conspiracy theories[47], disinformation related to core health issues (such as the COVID-19 pandemics or vaccination), political disinformation, etc. Certain practices may also have negative impacts on users' freedom to make informed political decisions and on authorities' capacity to ensure open political processes. Similar amplification tools, either through algorithmic recommendations or design 'dark patterns' can also tilt consumer choice on marketplaces and have an impact on sellers' ability to reach consumers[48].

43 This amplification happens through the design choices in platforms' ranking systems on embedded search functions, recommender systems, and through more or less complex advertising placement services, including micro-targeting.

44 Such issues stem from at least **two potential sources**:

45 *First*, structurally, **the optimisation choices** made by platforms in designing their systems and choosing the content amplified and matched with their users could, in themselves, lead to negative consequences. There is, for instance, debated evidence for the creation of 'filter bubbles' on social networks, where users are only exposed to

[44] A synthesis of relevant behavioural economy and psychology literature presented in (Lewandowsky & Smillie, 2020 (forthcoming))

[45] See, for example, (Alastair Reed, 2019) for a study on the recommender systems of three online platforms, pointing to some evidence on how theirs systems could prioritise right-wing extremism, including content that could qualify as illegal terrorist content

[46] https://ctc.usma.edu/christchurch-attacks-livestream-terror-viral-video-age/

[47] E.g. https://www.vice.com/en_us/article/d3w9ja/how-youtubes-algorithm-prioritizes-conspiracy-theories

[48] See, for example, potential trade-offs and welfare losses in using alternatively recommender systems and targeted advertising as marketing strategies in (Iusi Li, 2016) or https://webtransparency.cs.princeton.edu/dark-patterns/

certain types of content and of views, affecting the plurality of information they receive[49].

46 Micro-targeting with political advertising, for example, is also alleged to have similar effects, in particular in electoral periods[50], but evidence of actual impact in voter behaviour is not consistently conclusive[51]. Advertising can also be served in a discriminatory way, in particular where vulnerable groups are deprived from sensitive ads such as those related to access to goods or employment[52].

47 *Second*, as systems are dynamically adapting to signals they pick up from their users, they are vulnerable to manipulation by ill-intended individuals or organised groups. For example, bot farms are used to artificially increase traffic to certain types of content, either to drive ad revenue, or to fake the popularity of the content and trick the amplification algorithm into systematically ranking it higher. The behavioural aspects leading to abuse, as is the case in disinformation campaigns, go beyond the systemic issues analysed in this impact assessment.[53]

48 It is clear that the dynamics of online interactions have an impact on real world behaviours. However, extensive academic research[54], replies to the open public consultation from civil society, academics, some business associations and regulators pointed to significant shortcomings in the understanding and detection of risks and harms stemming from the amplification of information flows through recommender systems, ranking or advertising.

49 *First*, **users lack meaningful information** about how these systems function and have very little agency in their interactions with these systems. They are limited in understanding the source of the information, as well as its relative prominence. Direct information to consumers is also an issue for consumer choices, as illustrated by the EU Market Monitoring Survey 2019, which shows that in the market for holiday accommodations 62% of EU 27 consumers consider ranking of products in search results very or fairly important and 72% consider online reviews and comments very or fairly important for choosing goods and services[55].

50 *Second*, there are **very few ways of researching and testing the effects of such systems**. Much of the evidence and information about harms relies on the investigations and willingness to cooperate of online platforms themselves[56]. Some research projects and civil society experiments attempt to observe platforms' algorithmic systems and their

[49] Synthesis of the state of the art research in (Lewandowsky & Smillie, 2020 (forthcoming))

[50] For example (Jausch, 2020) or (Fundacja Panoptykon, 2020)

[51] See, for instance (Coppock, 2020) on limited effects of political advertising on voted behaviour, and (Jausch, 2020)

[52] See, for example, (Ali M., 2019) (Datta A., 2018)

[53] The latest assessment of the Code of practice on Disinformation details the more complex issues and the voluntary actions envisaged. https://ec.europa.eu/digital-single-market/en/news/assessment-code-practice-disinformation-achievements-and-areas-further-improvement This impact assessment does not address specifically, nor exhaustively, the issue of disinformation, but analyses a series of structural characteristics of online platforms which fuel such risks, along with other societal harms.

[54] See, for example, (Leerssen, 2020), or (Cobbe & Singh, 2019)

[55] https://ec.europa.eu/info/policies/consumers/consumer-protection/evidence-based-consumer-policy/market-monitoring_en

[56] E.g. voluntary partnerships with academics such as https://socialscience.one/ or reporting in the Code https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019 . Other cases concern platforms' own intentions to crowdsource the optimisation of its recommender systems, https://netflixtechblog.com/netflix-recommendations-beyond-the-5-stars-part-2-d9b96aa399f5

effects[57], but they require significant efforts to collect data, sometimes against the terms of service set by the platforms. They naturally focus on specific platforms. Such research and experiments fail to meaningfully observe and account for the iterative interactions between the learning systems, the online behaviour of users, and the governance set by the platforms, and cannot offer the continuous monitoring necessary to understand the systems.[58]

c) Fundamental rights are not appropriately protected

51 There is however an important balance to be struck between measures taken to remove illegal content and the protection of the fundamental right, especially freedom of expression and freedom to conduct a business. When platforms remove users' content, services or goods offered for sale, or de-rank them or otherwise limit access, or suspend user accounts, this can have severe consequences on the rights and freedoms of their users. This affects in particular their freedom of expression and limits access to information, but also on freedom of businesses and their ability to reach customers. These decisions are often not based on an assessment of the legality of the content, nor are they accompanied by appropriate safeguards, including justifications for the removal or access to complaints mechanisms, but they are solely governed by the discretionary powers of the platform according to the terms of services that are part of their contractual terms.

52 In some cases, content can also be removed erroneously, even if it is not illegal, nor in violation of the terms of service. Such cases can stem, for instance, from erroneous reporting by other users[59] and abusive notices, as well as from platforms' own detection systems, not least when automated tools are used. Notorious examples include takedown of historical footage used for educational purposes[60] or documented evidence from war zones[61].

53 Some regulatory initiatives, such as the Platform to Business Regulation[62], oblige online platforms to inform their business users of different aspects of their commercial relationship and provide those users with an effective complaint mechanism, as well as an out of court dispute settlement mechanism. Following the adoption of the revised Audiovisual Media Services Directive ('AVMSD')[63], for the specific area of audiovisual content on video-sharing platforms, other users will also have access to redress mechanisms to be set up by video sharing services, and to alternative out-of-court redress mechanisms to be set up by Member States.

---

[57] A short selection of examples includes: https://algotransparency.org and https://foundation.mozilla.org/en/campaigns/youtube-regrets/ for YouTube recommender systems, http://insideairbnb.com/about.html for data on AirBnB listings

[58] On the need for continuous, structural monitoring, see e.g. (LNE, forthcoming)

[59] (Urban, 2017)

[60] https://www.theguardian.com/technology/2019/jun/06/youtube-blocks-history-teachers-uploading-archive-videos-of-hitler

[61] https://www.wired.co.uk/article/chemical-weapons-in-syria-youtube-algorithm-delete-video

[62] 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

[63] 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

54 However, other users depend entirely[64] on the platforms' discretionary decisions as to whether they can have access to a complaint and redress mechanism. In the recovery steps of the COVID-19 pandemic, in particular, the effects of erroneous restrictions on businesses can be significant. Furthermore, the effectiveness of such systems varies greatly from one service to the other or from one type of content to the other. There is consistently a lack of redress and transparency of decisions unilaterally taken by the platforms. Very few online platforms subject their enforcement policies to systematic independent oversight (15 out of 61 service providers responding to the open public consultation).

55 It is virtually impossible to estimate in quantitative terms the **scale** of erroneous removals, blocks or restrictions. Very few online platforms report on the complaints they receive from users. Even fewer report on whether content is reinstated after such complaints are acted upon. Even then, such reports are not comparable, since they do not follow the same standards and criteria.

56 In the Eurobarometer survey run by the Commission in 2018[65], 5% of citizens responding said their content was erroneously removed, reaching 10% of respondents from Poland, 8% in Denmark, and 7% in Greece, Cyprus and Malta. 22% of the respondents concerned by the removals were not informed in any way about the reasons why their content was removed and 47% said they took no action to resolve the situation.

57 On many occasions, erroneous removals can have a **chilling effect on the users' freedom of expression** online beyond the specific content removed: in a survey[66] presenting theoretical takedown scenarios, 75% of respondents said they would be less likely to speak about certain topics online after their content is removed from a platform. More recent empirical research[67] has confirmed these behavioural changes on social networks. When marketplaces - which intermediate e.g. the sale of products of any type, accommodation services, transport services – take corrective measures against their sellers for alleged illegal activities, errors or ill-intended notices can have a **substantial adverse impact on individual businesses and traders**, in particular when these are largely dependent on these marketplaces and online channels for reaching their customers. On the other hand, a lack of effective procedures that may result in illegal content not being taken down may also have a considerable negative impact on fundamental rights, for example in the case of child sexual abuse material where known content re-surfaces and the harm is perpetuated.

58 Takedowns are potentially even more impactful when such measures are taken by services lower in the Internet stack, such as those providing the cloud infrastructure, web hosting, or content distribution network services, for instance. Actions taken in these cases can effectively disable access to entire services, blocking IP addresses, taking down full websites or rendering them inaccessible and/or vulnerable to Denial-of-Service attacks.

59 At the same time, fundamental rights are also at risk when users are prejudiced when service providers do not take any action, leaving content untouched that severely violates

[64] Some Member States have put in place voluntary mechanisms in partnership with individual platforms (e.g. Polish memorandum with Facebook) whereas others have included complaint mechanisms in their 'notice and action' national laws (see Annex 6)
[65] (Eurobarometer - TNS, 2018)
[66] (Penney, 2019)
[67] (Matias, 2020)

interests of others, including in cases where users have reported such content (see previous section a) here-above).

Who is affected and how?

60 The overall impacts of these problems are very broad and deeply connected to the various illegal activities themselves, and more broadly affecting behavioural patterns and functions of the online participation. It is outside the scope of the impact assessment report to present them in detail. As an illustration the most commonly reported issues referred to in the replies to the open public consultation are presented in the paragraphs below.

61 Illegal activities online have a serious impact on **safety and security online** which can also lead to offline consequences. CSAM content, and material that incite to terrorist acts or racists and xenophobic or gender-based violence affect important fundamental rights including the right to life and human dignity and the rights of the child. Other illegal activities can have an impact on **consumers**, which are affected by scams and misleading practices, or purchase dangerous and non-compliant goods. They can also affect legitimate businesses, either scammed themselves online, or as **manufacturers, brands, content creators and other IPR owners**, losing important revenues due to substitution of their offerings with illicit ones, as well as potentially suffering reputational damage. Illegal activities online also represent a competitive disadvantage for compliant businesses.

62 The proliferation of illegal content online can also have the effect of silencing speech, in particular where **vulnerable groups** are concerned. At the same time, erroneous removal of content can have important consequences on **citizens' freedom of expression**, as well as on businesses' ability to reach consumers and their **freedom to conduct business**.

63 When online intermediaries, such as online platforms, are concerned, the presence of illegal activities conducted by their users has controversial effects. In the public consultation, some respondents, in particular holders of IPR, flagged that illegal activities bring significant income to online platforms. At the same time, platforms and other intermediaries stated that when illegal activities are harming their users they may suffer reputational damage and loss of revenue, as well as incur legal risks from the service they provide. Recent developments, such as advertisers' walk-outs from certain platforms, point to the complexity of repercussions also on the intermediary's business practices and interests.

Stakeholders' views

In the open public consultation, a majority of respondents, all categories included, indicated that they have encountered illegal content, goods or services online, and specifically noted a spike during the Covid-19 pandemic. More specifically, 46% of the respondents to the relevant question indicated, that they had encountered illegal goods, and 67% of the respondents stated, that they had encountered illegal content online. Citizens and consumer organizations pointed to defective goods, counterfeits, fake event tickets, as well as significant issues related to hate speech, political disinformation and fake news. Business organizations and business associations raised the issue of online scams, as well as losses incurred due to intellectual property infringements. A large share of respondents who said they had notified illegal content or goods to platforms, expressed their dissatisfaction with the platforms' response, and the ineffectiveness of reporting mechanisms after the exposure took place. More specifically, 54% of the respondents, all categories included, were not satisfied with the procedure following the reporting, were not aware of any action taken by the platform as a follow up on their

reporting and consider that there is a lack of transparency following a notification. In addition, citizens pointed out, that notice and action procedures are very different from one platform to another, making the procedure of reporting illegal content/goods/services even more difficult and uncertain. Moreover, especially users and civil society organisations perceived there to be a mismatch between platforms' official policies and their concrete actions, and called for harmonised rules for digital services providers. Civil society organisations highlighted the significant information asymmetries between users and platforms, and academic institutions warned against the negative effects that amplification systems can have on the dissemination of illegal activities. With regard to the use of automated tools in content moderation, several respondents, especially business associations and online platforms pointed to both the usefulness and the limitations of such tools. There is a strong call for caution for obligations for the use of these tools due to risks of over removal of legal content by civil society organizations defending digital rights. Publishers, companies that sell products or services online, the general public, as well as digital users' and consumers' associations expressed concerns about the lack of transparency and accountability, especially in the context of targeted advertising and how algorithmic systems shape online content. Furthermore, the limited disclosure of ad content and the lack of ad targeting policy enforcement was flagged.

Moreover, whilst there is a strong call for action, many categories of stakeholders, including citizens, online intermediaries, civil society organisations, academic institutions and national authorities, emphasized that any new measure to tackle illegal content, goods or services online, should not lead to unintentional, unjustified limitations on citizens' freedom of expression or fundamental rights to personal data and privacy. Citizens, civil society organizations and consumer organizations pointed out the need for platforms to have a clear and transparent redress mechanism. Digital users' associations highlighted that the users have no way to appeal to anyone independent or neutral.

2.2.2. Ineffective supervision of digital services and lack of trust between authorities

In particular where online platforms are concerned, the supervisory system is to a large extent uncoordinated and ineffective in the EU, despite the strategic importance of such services. The E-Commerce Directive sets the internal market principle according to which the supervision of digital services is organised, but remains broad on the general principles for cooperation and information sharing across Member States. The perceived limitations in the day to day cooperation fuels a lack of trust across Member States when it comes to supervising online platforms in the interest of all EU citizens. In turn, this mistrust leads to an uneven protection of European citizens, and to uncertainties and lack of clarity for service providers.

64 Whereas online platforms and, to certain extent, online intermediaries at large, are misused for the harms presented here-above manifesting in different Member States, the current **supervision arrangements across the single market are not effective, and are insufficient in mitigating the evolving risks**. There are some sector-specific cooperation mechanisms which benefit from further specified procedures, such as in the area of consumer protection. However, overall there are several components fuelling this situation:

65 *First*, a core failure in supervision of digital services stems from the **lack of trust and cooperation** among authorities in cross-border issues. Online platforms are naturally

borderless, in particular where they reach a critical mass of users for a competitive service. The core principle of the single market aims at establishing the most effective supervision in order to safeguard the interests of all the European citizens. The country of establishment is best placed to take corrective measures against a service provider, while accommodating the cooperation with and assistance to authorities from other Member States[68]. For a smooth functioning of the system, Member States need to trust that digital services are effectively supervised at the source of the activity. To that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all citizens in the EU. At the same time, for the case of services such as online platforms, the underuse of the cross-border mechanism designed in the E-Commerce Directive, causes deficits in the supervision of online platforms and has eroded trust between Member States (see driver 2.3.6).

66 In both the open public consultation and the targeted consultation with Member States, the majority of authorities pointed to the increased importance of the cooperation across the single market. At the same time, they deplored the very limited use of existing channels, slow processes and response from other authorities, as well as the lack of clarity as to which cooperation mechanism should be used for specific and general issues. Some authorities emphasised the lack of a stable forum and incentives for Member States to share real progress and information. Further, they flagged the ever-increasing complexity of issues supervised at regional, national and European level, all sharing cross-cutting digital challenges, and the need to ensure the cooperation and transmission of information across these levels within and across Member States.

67 Absent an effective cooperation mechanism and as the risks have escalated with the scale and impact of online platforms, Member States have started to re-fragment the single market and legislate unilaterally to tackle these issues (see driver 2.3.1).

68 *Second*, **authorities lack information** and technical capability for inspecting technically complex digital services. This concerns both the supervision of the digital service and, in the case of online platforms in particular, the increasing challenges of supervising the underlying services they intermediate, such as accommodation or transport services, or websites conducting illegal activities online.

69 *Third*, authorities have very few levers for supervising services established outside of the Union, while such services are easily used e.g. for selling illegal goods or scamming consumers in the Union. Several authorities responding to the consultations launched by the Commission emphasised this grey area of regulatory supervision, where important services established outside the Union bear no legal obligations, whereas they reach a large number of Europeans.

Stakeholders' views

Several stakeholders groups, including public authorities, as well as different Member States pointed out that cooperation between authorities and enforcement is inadequate both cross-border and within each Member State. Member States, public authorities, civil society organisations and brand associations emphasized the need for the current system to be strengthened, and pointed to the knowledge gap, the inadequacy of existing cross-border mechanisms, and the lack of oversight and cooperation between all actors involved in the ecosystem as a key hindrance in effective oversight. Some national authorities considered that the country where a service is accessed does not have sufficient levers for enforcing its laws online. Businesses and business associations

[68] See Recital 22 of the E-Commerce Directive and further explanations in (Crabit, 2000)

bemoaned that regulatory oversight is neither clear nor foreseeable, and especially highlighted the regulatory burdens of complex, slow and bureaucratic procedures. Civil society groups referenced that the current governance approach is not broad enough and highlighted the need to cooperate with civil society organizations and academic as well as research institutions for specific inquiries and oversight, in particular where online platforms are concerned. Some civil society organizations flagged the absence of robust and effective enforcement mechanisms for regulatory oversight, in particular when it comes to fostering coordination between national authorities, and to address issues concerning the lack of transparency and inconsistencies within procedures. Similarly, the majority of respondents from academia pointed to the fact that platforms cannot credibly be held accountable without strong enforcement mechanisms. Finally, a majority of categories of stakeholders considered that in order to effectively supervise online platforms, rules should be applicable to third country players that are providing their services to European users. Online intermediaries stressed that any regulatory oversight mechanism should be proportionate, increase legal certainty, and follow a single market logic in ensuring the free provision of services.

2.2.3. Legal barriers for digital services, prohibitive for smaller companies to scale in the European single market

To address the challenges presented here-above, Member States have started regulating online platforms and online intermediaries at national level to supervise them and reduce harms. The resulting **legal burdens create new barriers in the internal market and lead to high direct and opportunity costs, notably for SMEs, including innovative start-ups and scale-ups**. This leads to a competitive advantage for the established very large platforms and digital services, which can more easily tackle higher regulatory compliance costs, and further limits the ability of newcomers to challenge these large digital platforms.

70 Some Member States are increasingly legislating to protect their citizens from those risks generated by online platforms established in a different Member State. When companies want to provide their services cross-border in the single market, they face a series of **regulatory burdens: legal fragmentation across Member States and legal uncertainties.**).

Figure 3 Online platforms in the EU

71 The impact on online platforms is asymmetric and **disproportionately affects small providers.** While larger online platforms are also subject to more costly obligations, those costs are still comparatively modest for them. In contrast, they can be prohibitive for start-ups and scale-ups attempting to provide services in several Member States and develop in the single market.

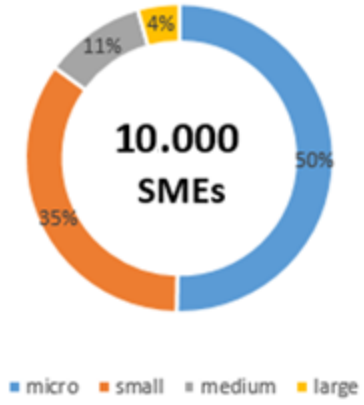
Cost of non-Europe

72 In a direct cost model[69], **company-level costs** stemming from the legal fragmentation range from EUR 31,000 to EUR 15 million per year for a small-sized enterprise (depending on the Member States where the company provides its services, as well as the overall volumes of content notified to them). For larger companies which also receive larger volumes of notices (from 200 to 3000 per day) and require a more robust infrastructure for processing them, costs can range from EUR 1,3 million to EUR 225

[69] Simulation of costs based expenditure data from publicly available reports from companies complying with the requirements in the NetzDG. See Annex 4

million per company. Simulating the effects of the ascending trend of legal fragmentation, all of these costs could double, should Member States continue to legislate in diverging ways. This model is only reflecting direct costs of the evolving legal fragmentation, accounting for the different rules on 'notice and action' obligations for online platforms, including the notification system, processing of notices, and, where required, availability of a counter-notice system, transparency requirements and the obligation to appoint a legal representative in different Member States.

73 With the evolving fragmentation, these costs can have an impact on the over 10,000 potentially high-growth platforms established in the EU[70], out of which around 96% are SMEs, more than half of which are micro-enterprises. For micro and small size enterprises, it is clear that the current costs are prohibitive for covering the entire single market. This is particularly concerning for digital services which typically need to draw on economies of scale to grow fast in order to secure their place on the market.



74 Across all sectors, the current state of the **legal fragmentation is estimated[71] to represent a loss of 1% to 1.8% in online trade** (i.e. modelled as cross-border use of online platforms, based on cross-border users for 31,084 web domains).

Legal uncertainty

75 Other legal burdens stem from the **uncertainties linked to the liability regime for online intermediaries** (see driver 2.3.5). This leads to a risk-avoidance behaviour in particular from small, emerging service providers, and decreases the quality of their service and their potential for a competitive edge, as testified by several service providers e.g. in their responses to the public consultation.

76 Consequently, direct costs from legal fragmentation are also accompanied by potential **opportunity costs** and missed potential for business innovation. In comparison to other countries, such as the US or China, the level of investment in European market places is significantly lower. However, scenarios based on data from venture capital investments show that there is potential growth for online platforms (16% increase in investment in 2019), in particular where platforms offer services linked to food, transport, fintech, travel, fashion, home, or enterprise software.[72] With increased compliance costs due to the growing legal fragmentation, the legal risks for start-ups and scale-ups have a chilling effect on investment and can dissuade businesses from expanding and growing in the single market.

Stakeholders' views

There is a convergence of views amongst business associations, companies, as well as Member States, that the current state of legal fragmentation of the Digital Single Market has created burdens for European businesses. These stakeholder groups see the trend of Member States enacting different legislations and rules around illegal content, goods

[70] Conservative estimates based on data available in the Dealroom database for 'hosting services' having received some venture funding or other external investment (September 2020)
[71] See annex 4 for an explanation of the model
[72] (Dealroom, 2020)

and services as limiting most businesses, but especially SMEs and start-ups, from scaling up. More specifically, business associations pointed out, that SMEs and start-ups are facing a competitive disadvantages, since they are affected in a disproportionate manner as opposed to larger companies. Start-ups and SME's pointed to the business risks of having to adapt their services to potentially 27 different MS-specific rules, which does not just inhibit their growth within EU borders, but also globally. Some business associations further explained that new digital services are often reluctant to expand in different European markets as a consequence of the diverging national legislations. More generally, 64% of respondents, all categories included, that replied to the relevant question in the public consultation considered the different processes and obligations imposed by the different Member States for notifying, detecting and removing illegal content, goods, or services as very burdensome, and 72% of respondents considered the different procedures and points of contact for obligations to cooperate with authorities as very burdensome. This issue is also recognised by national authorities, which support a horizontal harmonised framework to tackle fragmentation stemming from national and EU legislation.

Some intermediaries, national authorities, research institutes and civil society organisations consider that the current liability regime creates disincentives to act and call for the removal of disincentives for voluntary measures, in order to limit the risks of liability for intermediaries that voluntarily implement preventative measures to detect illegal content. Business associations and companies agreed, that the liability framework should be further developed in an innovation-friendly and uniform manner throughout Europe. Online platforms echoed the need for clear but proportionate rules and responsibilities that do not disincentive their voluntary actions to limit the distribution of illegal activities online. Some digital users' associations, trade associations and representatives of the creative industry fear that such clarifications could weaken the responsibilities of intermediaries, absent positive obligations.

2.3. What are the problem drivers?

2.3.1. Private companies make fundamental decisions with significant impact on users and their rights

77 Beyond responding to calls to remove content that is illegal, online platforms generally apply their terms of service and community standards, both for specifying what types of content and behaviours they allow, and by setting up the process for reporting and detecting non-compliant behaviours.

78 There is no oversight and generally an absence of checks and balances provided by law. This concerns equally decisions taken by service providers based on their terms of service, as well as measures put in place to tackle illegal activities following flags from third parties or proactive measures for detecting such activities. This leaves citizens' rights vulnerable. The opacity of this system also weakens the ability of authorities and law enforcement to supervise and pursue online crimes.

79 The very large online platforms generally have in place a system for notifying content, goods or services they intermediate, but the actions triggered are not always consistent. Other, smaller players do not support any notification system at all (two small service providers, out of 60 online intermediaries responding to the open public consultation did not have any such system). The rigor in analysing the reported or detected content varies.

Some studies[73] have shown that, when content is notified to platforms and the claim appears delicate or uncertain, they will likely remove the content to avoid risks of liability. This concerns in particular smaller online platforms, where business incentives to keep illegal content off their service are overthrown by the need to avoid legal risks. Conversely, parts of civil society, brand owners or authorities also complain that platforms are not systematically responsive to notifications about illegal content.

80 Further, platforms' own actions and tools for content moderation are not consistently accurate and there are very few possibilities to inspect the reliability of their systems. The largest platforms use both in-house and outsourced content moderation, including a range of technologies, from metadata and keywords trackers to infer illegal goods sold on their platforms, to fingerprint-based filters to detect illegal images previously identified, to machine-learning classifiers claiming to identify automatically certain types of content. The use of such tools, while promising in churning large volumes of content very fast, brings a set of challenges in particular with regard to more context-sensitive content. As concluded in a study commissioned by the European Parliament, *'such measures present significant drawbacks, including a lack of transparency concerning how the technologies work, a lack of adequate procedural safeguards and a risk of over-enforcement, with online providers being more likely to apply an algorithm that takes down too much rather than too little, content'.*[74]

81 Key components to safeguard users' rights, such as meaningful information to the user whose content was removed and to those that filed a notice, or an appropriate complaint mechanism, are also not consistently applied (three of the online intermediaries responding to the open public consultation), and are not equally reliable across services. 17% of respondents to a Eurobarometer survey,[75] whose content was erroneously removed by online platforms, also said that they were never informed by the platforms about the reason for the removal.

82 A quarter of the online intermediaries responding to the open public consultation said they did not have policies or identification measures for their business users established outside of the Union. Such measures are considered best practices[76] to dissuade illicit sellers and to enable the enforcement of sanctions against them. On-boarding processes for traders differ for each online marketplace: whereas some are asking for detailed information on the identity of the traders, others require a mere email address. Consumer protection authorities have also often reported their difficulties to enforce the law against rogue traders online due to the lack of information on the identity of such traders, especially when they are not established in the EU.

83 The large online platforms release **regular transparency reports.** This practice has increased since the Commission's Recommendation of 2018[77]. While it is important for such information to be released, not least as concerns requests from government authorities and content detected through user notices and proactively identified by the platform, these reports remain limited in scope and detail, making it difficult to understand to what extent illegal content, goods and services are appropriately identified

[73] (Urban, 2017)
[74] (Madiega, 2020)
[75] (Eurobarometer - TNS, 2018)
[76] (European Commission, 2020)
[77] Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online

and removed. They are not standardised, use different definitions and different metrics for the data reported, and can hardly be compared across services.

84 Some online platforms[78] are starting to set up additional structures in their decision-making on content moderation, with an oversight board formed of external experts, to judge on the most difficult user complaints against removal. Such structures have been praised as a sign of inclusiveness in making decisions with a societal impact, while at the same time criticised for the limited prerogatives given to the boards.[79]

2.3.2. Very large platforms can play a role of 'public spaces'

85 With the scale of some online platforms and their presence in increasing facets of our daily lives, they can sometimes be compared to **public spaces for expression and economic transactions**. They are key actors in facilitating the exchange of information and the exercise of freedom of expression on the internet, and consequently they present the highest societal and economic risks. With over half of the population in the EU using social media, reaching nearly 90% for those aged 16-24[80], the effects of the design and standards on these platforms have a wide reaching societal and economic impact. Over 50% of business use social media in Europe, in some countries this rises to nearly ¾ of all the companies established[81]. The main marketplaces attract millions of sellers, who depend on them for reaching their customers.[82] Product updates, product tests or errors can make or break entire revenue streams of companies whose traffic and visibility is to a substantial extent dependent on these platforms.

86 The overwhelming majority of users are centralised today in a small number of online platforms. While precise data on the number of users is not available, available data shows the staggering differences of scale in the reach of the few largest online platforms and the long-tail of other services.[83]

87 The business model of platforms is predominantly based on capturing the attention of users in the increasing volume of information, goods and services. These services operate to their benefit with strong network effects, economies of scale, and unmatchable access to user data. Reaching a certain number of users has enabled a self-fuelling exponential growth for a relatively small number of platforms, leading to an extreme concentration of users and market power. Ad spending for digital advertising has grown over 10 times since 2006, with 12.3% growth only in 2019 with a total of EUR 64.8 billion in Europe[84]. The revenues disparities based on online advertising streams are also staggering: search ads is consistently the biggest category of digital advertising, whereas video, social and mobile advertising are growing very fast.

88 The tools and mechanisms used to optimise engagement play a major role in shaping the information and goods we see, bringing with it a variety of risks and harms exasperated by the scale at which they operate. The recommender algorithms and tools developed for businesses and platform to capture the attention of users and consumers can have design

[78] Most prominently, https://www.oversightboard.com/
[79] https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_OTH_01_05_19.pdf
[80] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20190629-1
[81] https://www.statista.com/statistics/1090015/use-of-social-networks-among-companies-europe/
[82] Amazon, for example, is reported to host over 1.1 million business users in Europe cf. https://ecommercenews.eu/amazon-has-1-1-million-active-sellers-in-europe/
[83] See Annex 4
[84] Statista, based on IHS and IAB Europe data

flaws leading to unintended consequences with serious social impact[85], for example, studies have shown that algorithms on advertising-funded platforms prioritised disinformation in part because of its engagement rate and consequential attractiveness to advertisers[86]. At the same time, the systems can be 'gamed' to propagate illegal content and goods by malicious actors as well as to spread false narratives by way of computational propaganda: micro-targeting, bots, astroturfing[87] and search engine optimisation.[88]

89 The societal risk of exposure to illegal content and activities is particularly high on large online platforms reaching a very wide audience. Strategies of the largest platforms have enormous impacts on the safety of citizens and the fairness of businesses' commercial activities online. At the same time, tackling illegal content and the related harm on these large platforms is challenging because they have become public spaces for exchange of information and thereby freedom of expression in an ever-more digital society, without being responsible for any considerations of public interest.

90 Given these network effects and unmatched access to data, there is significant information asymmetry between large platforms, small businesses, citizens and public authorities. There is insufficient transparency and accountability around how design decisions of platforms have societal and economic impacts.

2.3.3. Legal fragmentation

91 The E-Commerce Directive sets the general framework for digital services established in the single market. The Directive harmonises the basic information requirements for digital services and liability exemption for online intermediaries. It does not prescribe procedures or obligations on service providers when it comes to the notification and removal of illegal content, but flagged already the need to explore such measures (Article 21 (2)).

92 Since the adoption of the Directive, the digital services evolved significantly, together with the scale of their use. Online platforms in particular pose increasing risks and challenges. To address this, in the absence of common rules, Member States are legislating unilaterally, fragmenting the single market and triggering a series of inefficiencies and ineffectiveness in the supervision and sanctioning of digital service providers.

93 The largest source of fragmentation comes from the rules established at national level for procedural **obligations for online platforms to address illegal information and activities conducted** by their users, as follows:

94 Nine Member States (Finland, France, Germany, Greece, Hungary, Italy, Lithuania, Spain and Sweden) have implemented a notice-and-action procedure in their legislative frameworks. For five of them this only applies to copyright infringements and related

[85] https://theconversation.com/facebook-algorithm-changes-suppressed-journalism-and-meddled-with-democracy-119446

[86] Avaaz (2019) 'Why is YouTube Broadcasting Climate Misinformation to Millions?' Available at: https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/ 19 Avaaz (2020) 'How Facebook Can Flatten the Curve of the Coronavirus Infodemic'. Available at: https://avaazimages.avaaz.org/facebook_coronavirus_misinformation.pdf

[87] A practice of manipulating messages or online campaigns, making it appear like they are stemming from 'grassroots' initiatives and supported by genuine participants, whereas they are sponsored and promoted centrally by organisations hiding their affiliation and financial link with the initiatives

[88] https://www.ivir.nl/publicaties/download/Report_Disinformation_Dec2019-1.pdf

rights thereof. In some (e.g. Germany) more recent laws apply specifically to certain categories of hate speech.

95 In several Member States (Finland, France, Hungary, Lithuania), minimum requirements for the notice are defined by law, to ensure that it is sufficiently motivated.

96 In Member States without statutory requirements for notices, the case law has provided indications concerning the content of the notice and the mechanism.

97 The precise requirements of these laws diverge to a large extent on several points: the minimum content of the notice, the possibility to issue a counter-notice, the timeframe to react to a notice, potential mandatory measures against abusive notices or the possibility to submit contentious cases to an independent third party. Consequently, the service providers concerned can be subject to a range of legal requirements, which diverge as to their content and scope.

98 In thirteen Member States, some form of opportunity to dispute the allegation exist. However, the situation in which counter-notices are possible differ greatly amongst Member States. For example, a counter-notice in Estonia is only possible when the removal order is ordered by a government agency. In Finland, Greece, Hungary, Ireland, Italy and Spain counter-notices are only possible in the context of copyright; and in Luxembourg, it is only possible during the merit procedure.

99 In eight Member States (Bulgaria, Estonia, France, Germany, Greece, Lithuania, Portugal and Sweden), some sort of alternative dispute settlement mechanism exist. For example in Portugal, there is an out of Court preliminary dispute settlement possible in case the illegality of the case is not obvious; in Estonia, a specific alternative dispute regime exists for copyright infringements, in which a specific committee can resolve disputes.

100 In addition, several, more recent laws were adopted or proposed, including a burdensome requirement for a service provider to appoint a legal representative in the respective Member State, even if already established elsewhere in the Union. This is the case in the German NetzDG, the French Hate Speech Law[89], the recently notified Austrian draft law to combat hate speech online[90], the German draft law to protection of minors[91] or the Italian "Airbnb" law[92].

101 Additional sources of fragmentation stem from the need for authorities, in particular at local level, to supervise and collect data related to accommodation services offered through online intermediaries (see Annex 6).

2.3.4. Regulatory gap: systemic issues are not appropriately addressed

102 In the last years, in response to various sector specific challenges, legislation has been adopted or proposed at EU level. For certain types of illegal or suspicious activities, recent EU legal acts include a series of targeted obligations on online intermediaries. They define specific legal obligations for issues such as copyrighted content[93], the sale of

[89] LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet

[90] Entwurf eines Bundesgesetzes über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz - KoPl-G)

[91] Entwurf eines Zweiten Gesetzes zur Änderung des Jugendschutzgesetzes; unofficial consolidated text: https://gameslaw.org/wp-content/uploads/Youth-Protection-Act-Draft-10.-Feb-2020.pdf

[92] DECRETO-LEGGE 24 aprile 2017, n. 50

[93] 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

explosive precursor chemicals[94], and other types of illegal products subject to market surveillance[95].

103 While all sector-specific legislative initiatives fulfil their aim to tackle the specific issues, important gaps remain on a horizontal level. None of these instruments provides fully-fledged rules on the procedural obligations related to all types of illegal content and the accountability and oversight mechanisms are by default limited to sector they regulate. In terms of scope, they are limited from two perspectives. First, these interventions address a small subset of issues (e.g. copyright infringements, terrorist content, child sexual abuse material or illegal hate speech, some illegal products). Second, they only cover the dissemination of such content on certain types of services (e.g. sub-set of online platforms for copyright infringements, only video-sharing platforms and only as regards audiovisual terrorist content or hate speech in the AVMSD).

104 With regard to online advertising services for example, the E-Commerce Directive sets a series of transparency and disclosure obligations on distinguishing the ad from other content, and on the identity of the advertiser, complemented by similar provisions in consumer law.[96] However, the provisions are limited to commercial communications and online advertising landscape has changed dramatically since the Directive was adopted.

105 For some categories of illegal content and activities, such as illegal hate speech, dangerous products or counterfeits, the Commission has facilitated self-regulatory mechanisms, including cooperation with national authorities and/or trusted third parties (e.g. the Code of conduct on hate speech[97], the Product Safety Pledge[98], the Memorandum of Understanding on the sale of counterfeit goods on the internet[99], the Memorandum of Understanding on online advertising and intellectual property rights[100]). These voluntary measures have been to some extent effective in terms of achieving effective removals and by fostering collaboration between Member States, platforms and civil society. They have, however, structural limitations in scope and scale: they are limited to the signatories of the measures and compliance with the agreed objectives cannot be appropriately supervised or sanctioned, given their voluntary nature.

106 The Recommendation of 2018 fleshed out procedural requirements that the sectorial legislation had not fully addressed. It included horizontal procedures for notice and action mechanisms, safeguards for users' rights and transparency.

107 These non-binding measures were only selectively applied by some services. For instance, several respondents to the open public consultation noted that reporting illegal goods is not easy for the majority of the users, both in terms of ease of finding the avenue for reporting as well as the procedure of submitting a report. Several hosting service

[94] Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors

[95] 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

[96] See annex 12 for a more detailed description of EU law framing online advertising

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

[98] https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/product-safety-rules_en

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

[100] https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-of-understanding-online-advertising-ipr

providers responding to the consultation said that they did maintain a system for users or third parties to flag illegal activities conducted on their service. Further, users have often reported that these mechanisms are very different from one platform to the other: the procedure can vary from a simple email to a complex portal, removal times vary and follow-up actions are not always provided. Furthermore, the Recommendation has not had a harmonising effect: Member States proposed legislation with diverging measures in the national legal drafts analysed so far.

108 As such, systemic elements remain unaddressed by the regulatory framework and the self-regulatory initiatives. There are no comprehensive rules across the single market, neither in national law (see driver 2.3.1), nor at EU level specifying the responsibilities of digital services, including online platforms.

2.3.5. Legal uncertainties and contradictory incentives

109 There are several sources of legal uncertainty for online intermediaries, as their business models or the underlying technologies have developed since the entry into force of the E-Commerce Directive.

Uncertainties

110 Over the years, an important area of legal uncertainty for digital service providers has been the scope of the definition of information society services. Especially in the area of collaborative economy, but also in the area of sales of goods online, the line between the online services, offered at a distance, and the underlying services, usually offered offline, has not always been clear. The consequences of the separation of these services are significant given that online services may fall within the scope of the E-Commerce Directive while the underlying services fall within sector-specific rules or horizontal EU legal acts, such as the Services Directive[101]. Operators have often mentioned such legal uncertainty as a source of concern for their growth. The relevant provisions of the E-Commerce Directive have been recently interpreted by the Court of Justice of the EU[102].

Liability regime for online intermediaries

111 The liability regime set in the E-Commerce Directive for online intermediaries is considered a cornerstone for allowing online intermediaries to emerge in the 2000s, but also to establish the right incentives for service providers not to be driven to interfere disproportionately with their users' freedom of expression, as well as the freedom of their business users.

112 *First*, the Court has interpreted the condition for hosting services to 'a passive and neutral role', as referred to in Recital 42 of the E-Commerce Directive for mere conduits and caching services[103] – and national courts have later on applied this case-law in contradicting ways. In this context, some national courts have equalled 'active role (of such a kind as to give it knowledge or control)' with a sort of **'appropriation'** of the

[101] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market

[102] For instance, UberPop was considered not to be an information society service (C-434/15), but Airbnb is (C-390/18).

[103] As pointed out by AG Jääskinen in his opinion in the eBay case (p. 139 ff): „As I have explained, 'neutrality' does not appear to be quite the right test under the directive for this question. Indeed, I would find it surreal that if eBay intervenes and guides the contents of listings in its system with various technical means, it would by that fact be deprived of the protection of Article 14 regarding storage of information uploaded by the users"

content (‘zu eigen machen’) to the extent that a reasonably informed user could conclude that the platform is the author or responsible for such content. Similar interpretation has been also proposed very recently by Advocate General Saugmandsgaard in a case which is currently pending before the Court[104]. When applied to hosting service providers, it is important to create legal certainty and ensure that this requirement cannot imply that automatic, algorithmic ordering, displaying, and tagging or indexing of the content it stores, activities that are today necessary to make such content findable at all, imply an active role.

113 *Third*, and related to this, the current regime entails some legal uncertainty, in particular for small players that might want to take measures for keeping their users safe, but, in order to escape legal risks, avoid doing so. The current legal framework under the E-Commerce Directive could be interpreted as creating contradictory incentives for service providers: proactive measures taken to detect illegal activities (even by automatic means) could be used as an argument that the service provider plays an ‘active role of such a kind as to give it knowledge of, or control over, the data’ controlling the content uploaded by their users, and therefore cannot be considered as to fall within the scope of the conditional liability exemption. This places small players, who cannot afford the legal risk, at a net disadvantage as compared to large online players which do apply content moderation processes to varying degrees of quality.

114 The transposition of the liability regime into national law has also generated some areas of fragmentation, as clarified in driver 2.3.3.

2.3.6. Limited cooperation among Member States and lack of trust

115 To ensure that under specific circumstances, Member States are able to adopt measures in respect of a given information society service, even if these would not be established within their territory but in the territory of another Member State, the E-Commerce Directive provides for a specific cooperation mechanism between Member States’ authorities.[105]

116 The number of notifications sent by host Member States to trigger the assistance from authorities in the Member State of establishment of a service provider is very low, benchmarked against the surge of cross-border online activities during the last decades. Since the transposition of the E-Commerce Directive there have been 141 notifications submitted through the cooperation mechanism (approximately 30 in the first 9 years after the entry into force of the E-Commerce Directive and 111 notifications from November 2013 and July 2020, through the Internal Market Information System (IMI system) provided by the Commission for electronic submission of requests from Member

[104] In case C-682/18 *YouTube.*

[105] The relevant provisions have been recently interpreted by the Court, who has confirmed that a Member State’s failure to fulfil its obligation to give notification of a measure restricting the freedom to provide an information society service provided by an operator established on the territory of another Member State, laid down in the second indent of Article 3(4)(b) of Directive 2000/31, renders the measure unenforceable against individuals, in the same way as a Member State’s failure to notify the technical rules in accordance with Article 5(1) of Directive 2015/1535 (judgment of 19 December 2019, Airbnb Ireland (C- 390/18, EU:C:2019:1112, paragraph 96). This judgment clarifies the legal effect the prior notification obligation by stating that it constitutes not a simple requirement to provide information, but an essential procedural requirement, which justifies the unenforceability of non-notified measures. The fact that a non-notified measure restricting the freedom to provide information society services is unenforceable may also be relied on in a dispute between individuals.

States)[106]. Only 18 of these concern online platforms, and mostly for consumer protection concerns.

117 In several surveys over the last years[107], Member States have expressed **dissatisfaction with several aspects of the existing cooperation mechanism.** These include the average timing for responses to Member States' requests, the quality of the feedback received, and the lack of clarity in the use of other cooperation and notification systems, such as the CPC. All these lead to **lack of trust** between Member States in addressing concerns about providers offering digital services cross-border, in particular where online platforms are concerned.

118 Further, the lack of trust fuels the tendency of Member States to regulate unilaterally. A **plethora of national laws** (see driver 2.3.3) regulating digital services are coming into force, which leads to **the fragmentation of the single market** and a limitation to the freedom to provide services, in particular when such laws have extraterritorial effect.

119 However, the complex set of issues that the socio-technical systems of online platforms and other digital services are posing cannot be adequately and thoroughly addressed on national level given the cross-border reach of platforms and relatively limited technical resources of national competent authorities. Member States shared that in their experience the existing knowledge gaps, the inadequacy of existing cross-border mechanisms, and the lack the cooperation between all actors involved in the supervision ecosystem, is a key hindrance in effective oversight of online platforms. These challenges were pointed out also in the European Parliament's resolutions[108] and, in the targeted and open consultations organised, some Member States have pointed to the opportunity of further mutual assistance and EU-level governance.

2.4. How will the problem evolve?

120 All the aforementioned problems can only be expected to become increasingly acute. The use of (some) digital services will only increase over time, and so will the risks of abuse and manipulation of these digital environments.

121 **Illegal and harmful behaviours** are consistently evolving. Perpetrators are seeking means to adapt to measures taken by service providers and authorities are active across a series of services or are migrating from larger to smaller platforms. In the current system, primarily based on sector-specific interventions and voluntary measures taken by service providers, interventions can hardly keep up with the agile ways in which services are abused. They will never cover all those services which can make a real difference, nor will they cover all categories of illegal content, goods or services.

122 Users will also continue to have virtually **no redress** when faced with removals or when their notice is left without action. In a context where more and more volumes of content are processed by online platforms, in particular the very large ones, decisions to remove, delist or otherwise restrict content will also become even more impactful for the rights of their users. In response to challenges with illegal content and societal harms, companies

[106] While MS are broadly satisfied with the IMI tool, there is a consistent confusion as to which cooperation mechanism should be used for which purpose (see ANNEX 8).
[107] 2019 Survey, 2020 targeted questionnaire, discussion in the e-Commerce Expert Group in October 2019.
[108] See Annex 13

will continue to deploy industry led initiatives, with limited safeguards and no public accountability or oversight[109].

123 **Member States will continue to legislate unilaterally and increasingly so with extraterritorial provisions,** in addressing the emerging challenges of online intermediaries. Legal uncertainty for service providers will increase, due to the increased fragmentation and the patchy interpretation of liability rules by national authorities. It is unlikely that the cooperation mechanisms currently in place will support the necessary coherence. The economic impacts on digital services, their business users and all citizens will be amplified.

124 A core issue in the online environment is the information asymmetry between service providers and authorities and the public at large with regard to the manipulation and abuse of their services by their users. Absent further intervention to rebalance this, the gap can only increase wider, weakening the capacity and capability of law enforcement and authorities to intervene. This will lead to a dangerous system, threatening the rule of law and the market balances.

125 Furthermore, with systems being increasingly capable of amplifying information online, the complexity and the impacts of these mediated information flows can only grow stronger, with severe repercussions on individual rights – such as non-discrimination and gender equality, right to freedom of expression and freedom to form opinions, privacy and data protection as well as the right to a high level of consumer protection– and more collective concerns – such as democratic participation, media pluralism.

2.5. Problem tree

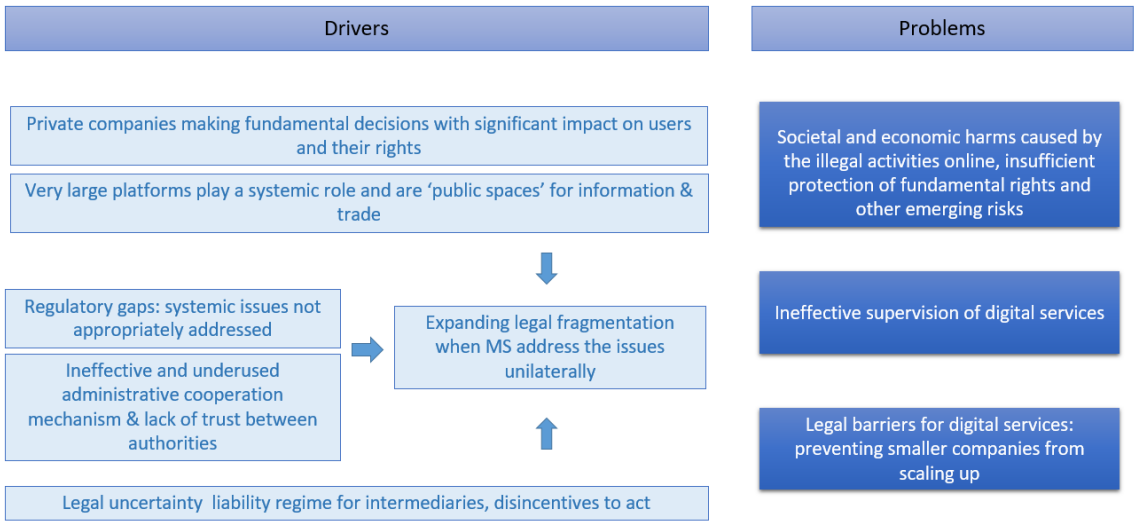


Figure 4 Problem tree

[109] For example, the Content Incident Protocol developed by the companies involved in the Global Internet Forum to Counter Terrorism, https://www.gifct.org/joint-tech-innovation/

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

126 Insofar as the EU intervention is likely to take the form of a legislative proposal, the legal basis depends on the primary objective and scope of the proposal. Legal intervention in the area of information society services with a primary goal of ensuring an internal market for these services could be based in Articles 53(1) and 62 TFEU (freedom of establishment and freedom to provide services), in Article 114 TFEU (approximation of laws for the improvement of the internal market) or in a combination of all these Articles. Articles 53(1) and 62 TFEU provide for the adoption of measures to coordinate the provisions laid down by law, regulation or administrative action in Member States on establishing and providing services. These articles allow only the adoption of Directives. Article 114 TFEU allows for the adoption of measures which are considered necessary for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market. These can take the form of a Regulation or a Directive.

127 The E-Commerce Directive, has a combined legal basis of Articles 53(1), 62 and 114 TFEU (Articles 47(2), 55 and 95 of the then Treaty establishing the European Community).

128 The primary objective of this intervention is to ensure the proper functioning of the single market, in particular in relation to the provision of cross-border online intermediary services. In line with this objective, the intervention aims to ensure the best conditions for innovative cross-border digital services to develop in the European Union, while maintaining a safe online environment with responsible and accountable behaviour of online intermediaries. To effectively protect users online, and to avoid that EU-based service providers are subject to a competitive disadvantage, it is necessary to extend the scope of the regulatory intervention to service providers which are established outside the EU, but whose activities affect the single market. At the same time, the intervention provides for the appropriate supervision of services and cooperation between authorities at EU level, therefore supporting trust, innovation and growth in the Digital Single Market.

129 The new legal instrument would build on the E-Commerce Directive with regards to the freedom of establishment and freedom to provide digital services in the single market, and further approximate rules applicable to intermediary services. Therefore, for either one of the policy options considered, the intervention can be solely based on Article 114 of the Treaty.

3.2. Subsidiarity: Necessity of EU action

130 According to the subsidiarity principle laid down in Article 5(3) TFEU, action at EU level should be taken only when the aims envisaged cannot be achieved sufficiently by Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the EU.

131 Several Member States have legislated on the removal of illegal content online in relation to aspects such as notice and action and/or transparency. This hampers the provision of services across the EU and is ineffective in ensuring the safety and protection of all EU citizens. The Internet is by nature cross-border. Content hosted in one Member State can normally be accessed from any other Member State. A patchy framework of national rules jeopardises an effective exercise of the freedom of establishment and the freedom

to provide services in the EU. Intervention at national level cannot solve this problem and has amplified the issues. The need to ensure the best conditions for innovative cross-border digital services to develop in the EU across national territories and at the same time maintain a safe online environment for all EU citizens are goals which can only be served at European level.

3.3. Subsidiarity: Added value of EU action

132 The different and diverging legal regimes applicable to online intermediaries increase compliance costs while also being the source of legal uncertainty as to the applicable obligations across the EU and leading to unequal protection of EU citizens. In addition, the effects of any action taken under national law would be limited to a single Member State.

133 EU action reducing compliance costs, allowing their predictability and enhancing legal certainty, while also ensuring equal protection of all EU citizens ensures that information society service providers' actions against illegal content online can be streamlined and scaled up, thereby increasing their effectiveness. This would oblige equally all companies to take action, and, as a result, strengthen the integrity of the single market. A well-coordinated supervisory system, reinforced at EU level, also ensures a coherent approach applicable to digital services providers operating in all Member States.

134 Action at EU level is only partially effective if it is limited to providers established in the EU. This creates a competitive disadvantage vis-à-vis companies established in third countries, which are not subject to any compliance costs in this regard. Furthermore, the effect on the availability of illegal content online is only limited.

135 Moreover, due to the interest of companies outside the EU to continue providing its services within the Digital Single Market, the EU can act as a standard-setter for measures to combat illegal content online globally.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objectives

136 The general objective of the intervention is to **ensure the proper functioning of the single market**, in particular in relation to the provision of cross-border digital services.

4.2. Specific objectives

4.2.1. Ensure the best conditions for innovative cross-border digital services to develop

137 The first specific objective is to establish the best conditions for the emergence and the scaling-up of intermediaries in Europe, by providing a predictable legal environment across the entire single market effectively addressing the current fragmentation, where the cross-border provision of services is as frictionless as possible and duplication of costs is limited. The aim is to ensure legal clarity and proportionality of obligations accounting for the differences in capability, resources but also impacts and risks raised by small, emerging services compared to very large, established ones.

4.2.2. Maintain a safe online environment, with responsible and accountable behaviour from digital services, and online intermediaries in particular

138 This objective is specifically linked to the first set of problems identified: the aim is to provide a framework of incentives and obligations which would facilitate a safe online environment for all citizens, for legitimate expression and for businesses to develop in observance of the rights and values of a democratic society. It aims at providing the legal clarity for online intermediaries, and in particular online platforms, to play their role in ensuring that their services are not misused for illegal activities and that the design of their systems does not lead to societal harms.

4.2.3. Empower users and protect fundamental rights, and freedom of expression in particular

139 Closely linked to the second specific objective, a modern online governance needs to place citizens at the centre and ensure that their fundamental rights and consumer rights are promoted. The aim of this objective is to ensure clear and proportionate responsibilities for authorities as well as private companies, to safeguard freedom of expression online by establishing rules that do not inadvertently lead to the removal of information that is protected by the right to freedom of expression and that speech is not stifled or dissuaded online. In particular, this objective seeks to enhance user agency in forming opinion and understanding their informational environment and enhance the protection of other fundamental rights such as the right to an effective remedy and to a fair trial, non-discrimination, protection of personal data and privacy online, rights of the child, etc.

4.2.4. Establish the appropriate supervision of online intermediaries and cooperation between authorities

140 None of the other specific objectives can be achieved without appropriate supervision and accountability of services, to ensure trust in the digital environment, and to guarantee online safety and the protection of rights. This necessarily requires some level of transparency of digital services, as well as appropriate capabilities and competence for authorities to supervise. This also requires the best possible cooperation and trust amongst authorities in all EU Member States, ensuring both an effective supervision and creating the best conditions for innovative services to emerge, as per the first specific objective.

4.3. Intervention logic

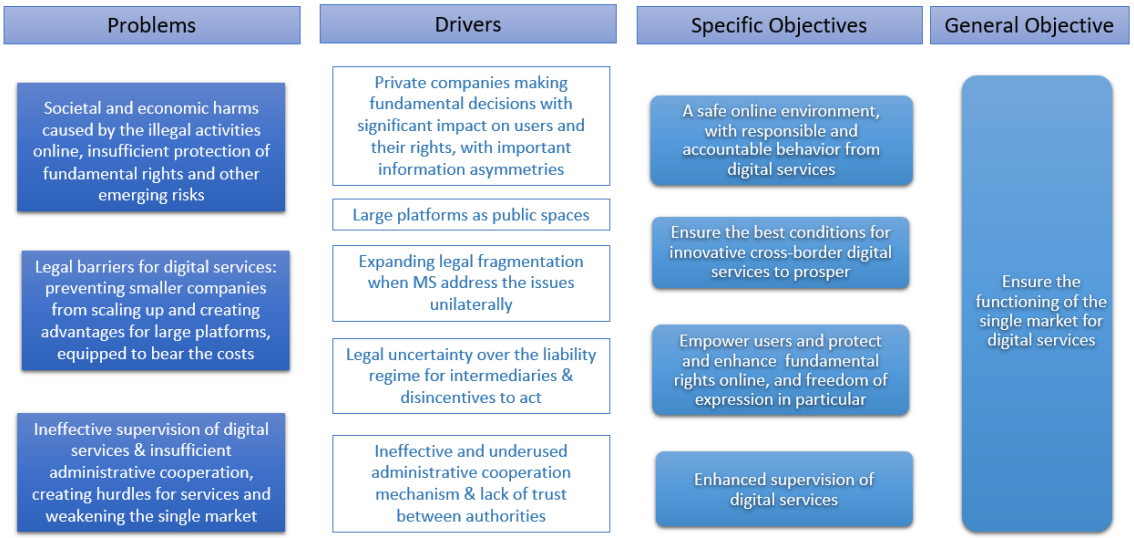


Figure 5 Intervention logic

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1. What is the baseline from which options are assessed?

141 **In the baseline scenario,** the Commission would not propose any changes to the current legal framework and keep enforcing the E-Commerce Directive. The Commission would monitor the take-up of the Commission's Recommendation on measures to effectively tackle illegal content online, and the transposition of sector-specific interventions such as the Directive on Copyright in the Digital Single Market, the recently amended Audiovisual Media Services Directive and the Terrorist Content Regulation, once adopted.

142 The Commission would also **continue to facilitate the coordination of self-regulatory measures targeting some types of illegal activities**, such as the dissemination of illegal hate speech, terrorist content, dangerous or counterfeited products, etc. Further action could focus in particular on more self-regulatory actions, which are naturally limited to some services participating on a voluntary basis, and with limitations regarding the enforcement or monitoring of the results. Courts would continue to interpret the obligations of new digital services against the framework of existing EU law as regards the concepts of 'information society services' or 'intermediary services' of the E-Commerce Directive.

143 In the absence of further EU legislation, and subject to enforcement of the current legal framework, legal fragmentation in areas not yet subject to sector specific legislation is likely to increase. Already today, a number of Member States, such as Germany, Austria, Denmark or France, have adopted or are in the process of adopting new laws to regulate digital services. A patchwork of national measures would not effectively protect citizens, given the cross-border and international dimension of the issues.

144 The proliferation of illegal goods sold online and the dissemination of illegal content would likely continue. At the same time, there would be no harmonised safeguards established for protecting users' fundamental rights and against over-removal of legal content. Tools for understanding and mitigating cross-sectoral societal concerns and the

economic impact of information 'acceleration' online would remain limited to incidental and incomplete experiments by researchers and civil society.

145 A notable inherent risk of the baseline scenario is the ongoing rapid evolution of the digital environment itself. Companies are setting and enforcing the rules themselves, driven by their commercial interests and not addressing consistently the societal concerns inherent to the digital transformation they are enabling. The ever-growing information asymmetry between online services and their users or the authorities is already making it very difficult to enforce rules online and to supervise the evolving challenges and risks.

146 In the baseline scenario, there is no palpable indication that the trend in increased availability of illegal content, goods or services offered online could be curved, in particular where sector-specific legislation is absent. While some platforms will continue to deploy measures according to their own policies, others, in particular smaller players, will continue to be dissuaded by the lack of legal certainty. Further, without harmonised standards on the responsibilities and actions expected from service providers, their approaches will consistently fail to offer a reliable due process standards for users' rights. This will continue to be a particularly acute issue where very large platforms are concerned, where the information asymmetries and the negotiation disparities with their users are the biggest, and where erroneous decisions are likely the most impactful.

147 Barriers for promising European Union companies to scale up in the single market would increase, reinforcing the stronghold of large online platforms, and reducing the competitiveness of the internal market.

5.2. Description of the policy options

148 A wider set of options was considered at the scoping phase of the impact assessment, in particular in relation to: the obligations placed on online intermediary services and in particular on online platforms, the liability regime of online intermediaries, their supervision across Member States, and a longer list of issues flagged in the European Parliament's own initiative reports on the Digital Services Act. Discarded options are presented in more detail in section 5.3 below.

149 In addition to the baseline, three packages of options are retained for assessment. They each include a different package of harmonising measures for the due diligence obligations to service providers and a regulatory supervision system appropriate to enforce these measures, as well as updates to the liability regime for online intermediaries. Each of the options is constructed to complement, but not to amend sector-specific legislation, and assumes the continuance and reinforcement of self-regulatory and voluntary efforts compared to the baseline. They all preserve and follow the core principles and provisions of the E-Commerce Directive, including the internal market principle for the supervision of digital services, the approach to the liability exemption for online intermediaries and the prohibition of general monitoring obligations or general obligations on online intermediaries to seek facts and circumstances for illegal activities. Options 2 and 3 make some amendments to the application of the liability regime.

150 The three retained options are the following:

1. Limited measures against illegal activities, laying down the procedural obligations for online intermediaries and in particular online platforms, to tackle illegal activities, in order to protect users' fundamental rights and ensure

transparency. It would also enhance the cooperation mechanisms for authorities to resolve cross-border issues related to the supervision of the rules.

2. Fully harmonised measures to incentivise actions from service providers, to enhance transparency and address a wider set of emerging risks by empowering users. Enforcement and cooperation mechanism enhanced with the appointment of a central coordinator in each Member State.
3. Asymmetric measures with stronger obligations for very large online platforms, further clarifications of the liability regime for online intermediaries and an adapted EU governance system to supervise the new obligations on very large online platforms.

Table 2 Summary of options considered in addition to the baseline

	Option 1 ***Limited measures against illegal activities***	***Option 2*** ***Full harmonisation***	***Option 3*** ***Asymmetric measures and EU governance***
Obligations on online intermediaries, in particular online platforms	**Due diligence obligations** for a fit and proper operation, including notice & action, know your business customer, transparency of content moderation, cooperation with authorities, clear terms and conditions including respect for fundamental rights	**Due diligence obligations**, including notice & action, know your business customer, transparency of content moderation, cooperation with authorities, clear terms and conditions including respect for fundamental rights, as well as transparency towards users on advertising	**Due diligence obligations**, including notice and action, know your business customer, transparency of content moderation, cooperation with authorities, clear terms and conditions including respect for fundamental rights, as well as transparency towards users on advertising **Enhanced responsibilities for very large online platforms** to mitigate systemic risks: e.g. reporting and data access to researchers and regulators, independent systems audits, appointment of a compliance officer, accountability of executive boards, participation in co-regulatory efforts to mitigate emerging risks and report on outcomes
	Sector-specific interventions through self-regulatory measures	Sector-specific interventions through self-regulatory measures	
Liability of intermediaries and injunctions	Baseline (rely on **case law**)	Remove disincentives for **services to take action** Harmonise conditions for **court and administrative orders** for removal of illegal content	Clarifications for **new types of services** in the Internet stack not clearly fitting in the categories of the E-commerce Directive Clarification where a service cannot benefit from the liability exemption Remove disincentives for **platforms to take action** Harmonise conditions **for court and administrative orders** for removal of illegal content and data requests

Supervision	**Enhanced administrative cooperation (digital clearing house)**	**Central 'coordinator' in each Member State** **Digital clearing house**	**Sub-option 3. A: EU Board as an advisory committee formed of representatives of digital services coordinators from Member States.** COM powers to apply sanctions **Sub-option 3.B: EU Board as a decentralised agency with investigatory and sanctioning powers** **Digital clearing house**

1. **Option 1 – Limited measures against illegal activities**

151 The first policy option establishes a set of **due diligence obligations** for tackling illegal activities online, essentially building upon the Recommendation of 2018 and the E-Commerce Directive. The measures apply to any type of illegal activity, as defined in EU and national law. The core elements of the due diligence obligations include the following:

- **Notice and Action** – Obligation to establish and maintain an easy to use mechanism for notifying any illegal content, goods or services offered through online platforms as well as other hosting services in accordance with harmonised standards. This is coupled with an obligation to inform users if their content is removed, including when the removal follows an assessment against the terms of service of the company, as well as specific actions around repeat offenders. The information obligations are coupled with an obligation to put in place **an accessible and effective complaint and redress mechanism** supported by the platform and the availability of an external out of court dispute mechanisms.
- **Know Your Business Customer ('KYBC')** – Online platforms that facilitate transactions between traders and consumers have an obligation to collect identification information from traders to dissuade rogue traders from reaching consumers.
- **Transparency obligations** – Regular transparency reporting on the measures taken against illegal activities and their outcomes, including removal rates, complaints, and reinstatement of content, transparency of the use and functioning of automated tools for content moderation, if applicable.
- **Cooperation obligations –** Obligations to cooperate with organisations designated as trusted flaggers by applying fast-track procedures for notices.
- **Fundamental rights standards in terms of service –** This includes the obligation to clearly state in their terms of service any restrictions they may apply in the use of their service, and to enforce these restrictions with due account to fundamental rights.

152 Self-regulatory measures through codes of conduct would continue to be encouraged and supported by the Commission and, further measures could be launched, as necessary.

153 Concerning the supervision of digital services, this option would build on the cooperation mechanisms established in the E-Commerce Directive and further develop a **'Digital Clearing House'** to facilitate the exchange of information among Member States and channel requests regarding failures of a given service provider to comply with the applicable requirements. This would cover both information from the country of establishment on sanctions imposed, and requests from authorities in other Member States. Member States can designate one or several authorities competent for supervising the new obligations.

154 The scope of the due diligence obligations would be extended to all services targeting the European Union, regardless of their place of establishment. For supervising and enforcing the due diligence obligations, a requirement for a legal representative in the Union would be imposed on services with a significant number of users in one or several Member States.

Stakeholders' views

There is a strong call for action throughout all categories of stakeholder groups and a consensus that certain responsibilities (i.e. legal obligations) should be imposed on online platforms. For instance, a large majority of stakeholders that answered to the public consultation want all platforms to be transparent about their content policies, support notice and action mechanisms for reporting illegal activities, and request professional users to identify themselves clearly (90%, 85% and 86% respectively).

As regards the nuances between the different stakeholder groups regarding due diligence obligations, the general public, online intermediaries and civil society organisations especially advocated for a harmonisation of notice and action procedures across the EU, and businesses called for the establishment of minimum information requirements for a notice to be actionable. Civil society organizations and the general public stressed the importance of human moderators. Furthermore, most contributions of media and audiovisual associations argued for the need of clear policies against 'repeat infringers', and also for the regulation of the notion of 'trusted flaggers'. The majority of retail associations highlighted the need for platforms to inform consumers who have previously bought an illegal or dangerous product that they have been exposed to illegal goods. Concerning online marketplaces, many stakeholder groups flagged the need to verify the sellers in order to provide transparency to consumers, and to increase the efficiency of enforcement. Especially rights holders and brands stated that they are incurring considerable costs by having to identify fake listings, and for reporting the sale of counterfeit goods or other illicit products to platforms.

Regarding supervision, 85% of respondents who replied to the relevant question in the OPC on the DSA package (2020), think that online platforms cannot be trusted to sufficiently guarantee democratic integrity, pluralism, non-discrimination, tolerance, justice, solidarity and gender equality. A large majority of stakeholder groups called for improved cooperation between authorities in different Member States and highlighted the importance of data sharing with law enforcement authorities, in particular for rogue traders. Member States flagged the challenges of consumer protection authorities regarding the effective enforcement to tackle illegal or shady business practices, and point to a low level of awareness among the enforcement bodies and a lack of harmonization of EU law. Some Member States further called for the current cooperation system to be revised and strengthened in order to avoid a fragmentation of the European digital market. They stated, that the emerging patchwork of EU and national legislation makes it even more challenging for enforcers to oversee the European market. Online intermediaries emphasized the importance of coordination between national authorities

and between all actors involved in the ecosystem.

2. Full harmonisation

155 This option would include the same due diligence obligations as those foreseen in option 1.

156 In addition, this option would impose on online platforms further transparency obligations towards their users, specifically regarding advertising systems – modernised transparency obligations covering **all types of advertising** (all ads placed on online platforms, not just commercial communications, but also e.g. issues-based or political advertising). Such measures would include enhanced information to users distinguishing the ad from 'organic' content, information about who has placed the ad and information on why they are seeing the ad (depending on the type of advertising – e.g. targeted, contextual - and, if applicable, targeting information).

157 This option harmonises certain conditions for cross-border court or administrative orders to impose measures for the removal of illegal content, goods or services by intermediaries.

158 In this option as well, self-regulatory measures through codes of conduct would continue to be encouraged and supported by the Commission and, further measures could be launched, as necessary.

159 Concerning the **liability of intermediaries**, option 2 would adapt the existing legal framework to remove disincentives for services, in particular online platforms, to take voluntary measures to address illegal activities: the intervention would clarify that such measures do not, in themselves, remove intermediaries from the scope of the liability exemptions.

160 Regarding the **supervision of digital services**, this option would complement the first option's Digital Clearing House by requiring Member States to designate a supervisory authority as a central Digital Coordinator. The Digital Coordinator would be tasked with facilitating coherence of the supervision and enforcement across different authorities in the relevant Member State, not least as regards capabilities and supervision of the additional obligations related to algorithmic systems in recommender and advertising systems, as well as with ensuring the cooperation interface for smoother cross-border assistance through the Digital Clearing House.

Stakeholders' views

In addition to the broad convergence around the core due diligence obligations also presented in option 1, a variety of stakeholder groups voiced concerns around online advertising, more specifically the lack of user empowerment, especially as regards deceptive advertisements, and lack of meaningful oversight and enforcement. Users demanded that reporting deceptive advertisements should be facilitated, both, when the advertisement is encountered online, and after the fraud was discovered by the user. The most frequent issues pointed to as necessary relate to more transparency regarding the identity of the advertiser, how the advertisements are personalized and targeted, and to the actions taken by ad intermediaries to minimize the diffusion of illegal ads and activities. Implementing features that explain why certain advertisements are shown to users were considered a good practice to build upon and to empower users.

Some intermediaries, academic institutions, and civil society organizations stated that the current liability regime creates disincentives to act, and called for clarification to stimulate voluntarily preventative measures to detect illegal content. Especially the

absence of incentives are seen as counter-productive in the fight against illegal activities online. Start-ups strongly supported the removal of disincentives for voluntary measures and stressed that this would be a very important safeguard for smaller online platforms and would incentivize businesses to take voluntary actions. Start-ups converge on the opinion that illegal content should be tackled by all online platforms regardless of their capacity, whereas harmful content should not fall under this regime. They are proponents of making all platforms introduce clear terms and conditions, and to develop best practices. Consumer organisations strongly called for a special liability regime for online market places to make them directly or jointly liable in case they exercise a predominant influence over third parties or in case the platform fails to properly inform consumers or fails to remove illegal goods or misleading information (assessed in Annex 9).

Online intermediaries generally considered that any new measure should avoid being overly prescriptive as regards the use of specific tools or technologies in the context of content moderation. In this context, stakeholders, especially civil society and digital rights associations, warned against monitoring requirements and the use of automated tools for tackling illegal or harmful content, goods and services due to significant risks to citizens' fundamental rights, right to privacy, and freedom of expression. 82% of all stakeholders that answered to the relevant question in the public consultation, support high accuracy and diligent control mechanisms, including human oversight when automated tools are deployed for detecting content or accounts. Start-ups, scale-ups and smaller platforms pointed out that automated tools are also very costly to develop and maintain, and see this as a significant barrier to market entry.

Member States stated that while the cooperation between authorities and larger service providers has provided for some good results, a more formal regulatory framework and an update to the current legislation is desired. Many Member States pointed to the risks related to the inability to provide effective surveillance and enforcement on the global digital services environment. Member States also warned that the digital single market should not be overregulated. Medium-sized and smaller companies, as well as business associations, flagged the fragmented state of the digital single market as a burden in providing digital services, especially when expanding to one or more Member States. Mentioned were especially the requirement to have a legal representative or establishment in more than one Member State, and the different procedures and points of contact for obligations to cooperate with authorities. When asked what governance arrangements would lead to an effective system for supervising and enforcing rules on online platforms in the EU in particular as regards the intermediation of third party goods, services and content, 81% of stakeholders called for a cooperation mechanism within Member States across different competent authorities responsible for systematic supervision on online platforms and sectorial issues. 80% of respondents stated that a cooperation mechanism would need to have swift procedures and assistance across national competent authorities across Member States. National authorities are also in favor of a reinforced cooperation mechanisms, but some call for assessing the effectiveness of a European agency. Some civil society organisations emphasized that robust and effective enforcement mechanisms for regulatory oversight are absolutely necessary, in particular to foster coordination between national authorities and to address issues with lack of transparency and inconsistencies within procedures.

3. Asymmetric measures and EU governance

161 The third option retains all the components of Option 2, but includes an asymmetric regime, targeting those very large platforms where the biggest audiences are reached – and, potentially, the most severe harms are caused.

162 **Very large platforms** represent the highest societal and economic risks because of their significant reach among citizens and traders in the EU. Therefore, the definition of very large platforms in this option is based on the number of users, as a direct and objective proxy for their reach and potential impact. The threshold is set at 45 million monthly users from the EU, the equivalent of 10% of the EU population. Available data shows that the largest online platforms captured by this threshold correspond to the services considered by stakeholders and academics to represent the highest societal and economic risks, and typically have a pan-European presence. Also, the providers of these online platforms generally have a high turnover and/or market capitalisation value. The platforms' reporting obligations and the Digital Services Coordinators' enquiring powers will ensure that the data on the number of users is available to enforce the enhanced obligations. As explained in more details in Annex 4, other alternative and cumulative criteria have also been assessed and discarded for the purposes of the definition of very large online platforms.

163 The **additional set of enhanced obligations on very large online platforms reaching a significant number of Europeans** are designed proportionately to the systemic impacts and risks these large platforms represent for society and the business environment, as well as to their capacities. Their due diligence obligations are obligations of means, without an expectation of no-fault results. These enhanced obligations are necessary to secure compliance with the rules ensuring the safety of citizens and the prevention of deceptive and fraudulent commercial practices online. This includes:

- obligations to maintain a risk management system, including annual risk assessments for determining how the design of their service, including their algorithmic processes, as well as the use (and misuse) of their service contribute or amplify the most prominent societal risks posed by online platforms. An obligation to take proportionate and reasonable measures to mitigate the detected risks follows, and the risk management system is regularly submitted to an independent audit;
- enhanced transparency and reporting obligations with regard to content moderation, content amplification and online advertising activities at the request of competent supervisory authorities;
- user-facing transparency of content recommender systems, enabling users to understand why, and influence how information is being presented to them;
- obligations to ensure access to data for researchers for investigations into the evolution of risks;
- maintenance and broad access to ad archives;
- a renewed co-regulatory framework with participation in adaptive and responsive codes of conduct to mitigate emerging risks coupled with an obligation to ensure reporting on outcomes and participation in crisis management protocols, responding to extraordinary situations where risks manifest online.

164 Option 3 includes, apart from the removal of disincentives to voluntary actions, as per Option 2, further **clarifications of the liability regime for online intermediaries** to ensure **legal certainty and innovation.** It addresses the fragmentation stemming from the different national approaches to the liability exemptions and preserves the principle of conditional liability exemption. To afford more legal clarity in grey areas of

interpretation concerning online platforms, it also specifies the conditions under which such services are truly intermediaries.

165 Similar to option 2, option 3 harmonises certain conditions for cross-border court or administrative orders to impose measures for the removal of illegal content, goods or services by intermediaries. Additionally, it includes obligations to notify of suspicions of criminal offences, where an intermediary service becomes aware of any information[110]. Furthermore, it also includes conditions for cross-border orders for competent authorities to access data necessary for supervising underlying services intermediated by online platforms.

166 For the **supervision of the obligations**, next to the Digital Clearing House and the national Digital Coordinators, an EU Board, including the participation of the national Digital Services Coordinators, enhances the governance system, particularly necessary for ensuring the supervised risk management approach for very large platforms. This system ensures in particular that systemic problems brought by those platforms with an EU-wide impact are appropriately addressed through EU supervision, with sufficient expertise and appropriate competencies, which is based on the clarified powers of the host Member State and rules for cooperation with the other Member States. It ensures appropriate assistance from other Member States and the Commission to the Member States in charge of supervising very large platforms. Building on the enhanced data access obligations for very large platforms, this includes in particular the technical assistance for complex investigations related to algorithmic systems or language-specific issues. This system also provides for fast information channels for all Member States where the effects of platforms' content moderation decisions are felt. Further, it provides for an escalation system where the Commission can supervise and take direct enforcement measures against very large platforms. Sanctions applied would be proportionate to the severity of the systemic non-compliance.

167 This options considers two approaches, distinguishing the legal form of the EU Board:

- **Sub-option 3.A**: the EU Board is established as an ad hoc independent advisory group, advising Digital Services Coordinators and the Commission on supervisory and enforcement issues, including those related to very large platforms (inherently present across Member States).
- **Sub-option 3.B**: the EU Board is established as an EU body with legal personality, supported by a secretariat and, in addition to the powers under sub-option 3.A, it can also adopt binding decisions.

Stakeholders' views

Whilst there is a general call, especially among citizens, for establishing as much transparency as possible, most stakeholder groups, especially business organisations and start-ups stated that not all types of legal obligations should be put on all types of platforms. Press publishers, for example, state that due diligence obligations should only concern very large online platforms, and should not cover hosting services such as comments sections on newspapers' websites. A majority of stakeholder groups, including business associations, academic institutions and the general public, recognized that not all platforms should be required by law to cooperate with national authorities, but that platforms at particular risk of exposure to illegal activities by their users should maintain a system for assessing the risk of exposure to illegal content or

[110] This does not imply an obligation to actively to seek facts or circumstances indicating illegal activity

goods and be required to systematically respond to requests from law enforcement in accordance with clear procedures as well as employ appropriately trained and resourced content moderation teams. 72% of respondents to the relevant question in the public consultation consider both, independent system audits and risk assessments as essential, especially when it comes to countering the spread of disinformation, as well as reporting and data access to researchers and regulators. How algorithmic systems shape online content is an area of concern among a wide category of stakeholders. Several stakeholders, amongst them citizens, civil rights organizations, academic institutions as well as media companies and telecommunication operators pointed out the need for algorithmic accountability and transparency audits on very large platforms, especially with regards to how content is prioritized and targeted. Users should receive more information and have more control over the content they interact with and digital rights associations think they should be able to opt out of micro-targeting and algorithmically curated content.

Academic institutions pointed to persistent difficulties when conducting research, and explained the difficulty of observing emerging issues and phenomena online, blaming an inconsistent access to relevant data. Some pointed to the need for a generally disclosed ad archive, as well as an independent auditing of ad systems. According to start-ups and SMEs, limiting some obligations to large players would ensure that the legal obligations are targeted to where problems actually occur. Start-ups especially stressed the point that a 'one-size-fits-all' approach would be most beneficial for very large platforms, but could have detrimental effects on medium-sized or smaller platforms and businesses at the core of the European digital ecosystem. They stress that their growth and evolution should not be hindered by disproportionate rules that impede on the successful development of competing alternative services and business models. Online intermediaries acknowledged the possibility of more transparency, but warned against possible implications of far-reaching measures in terms of compromising commercially-sensitive information, violations of privacy or data disclosure laws, and abuse from actors that could game their systems. Some online intermediaries considered that a transparency obligation could be best achieved by establishing a requirement for regular reporting.

Start-ups, telecommunication operators and several other stakeholders, notably new types of services in the internet stack, such as cloud services, CDN and DNS services, as well as other technical infrastructure providers, called for clarifications in the liability regime of intermediaries, without challenging its basic principles. Small companies in particular deplored the lack of legal predictability with regard to voluntary measures they might take. They also called for due diligence obligations on hosting service providers, and proportionate and targeted measures.

An effective EU oversight is considered essential for the compliance with the due diligence obligations by most stakeholder groups, especially telecommunications operators. Many stakeholder groups, but especially business associations and companies, considered, that the degree of oversight should vary depending on the services' obligations and related risks. The majority of stakeholders groups favoured a unified oversight entity to enforce rules on digital service providers (66% of the respondents to the relevant question in the public consultation. Authorities called for a coordination and technical assistance at EU-level for supervising and enforcing rules on online platforms as regards the intermediation of third-party goods, services and content.

Especially in the context of addressing the spread of disinformation online, regulatory oversight and auditing competence over platforms' actions and risk assessments was

considered as crucial (76% of all stakeholders responding to the relevant question in the public consultation. Academic institutions as well as civil society organizations showed concerns about the lack of adequate financial and human resources in competent authorities tasked with supervision of digital services. Many groups of stakeholders, especially civil society organizations defending digital rights, identified the need for interdisciplinary skills in a new oversight entity, particularly in-depth technical skills, including data processing and auditing capacities, which would allow for the reliable and thorough assessment of algorithmic abuses. The majority of academia and civil society organizations defending fundamental rights consulted, emphasized the need for strong, proportionate and foreseeable enforcement to hold platforms to their promises and are in favour of a supervised regulator or authority, to reconcile opposing needs and potentially sanction repeated failures.

5.3. Options discarded at an early stage

168 The options selection followed a funnelling methodology, exploring the widest spectrum of approaches. Several types of options were discarded earlier in this process, as explained below. In several cases, the assessment of the impacts on fundamental rights led to the discarding of these options because they did not ensure a fair balance in mitigating the risks.

169 Continuing to only regulate on a **sector-specific approach**, as done e.g. for content infringing copyright, terrorist content, explosive precursors, audiovisual content: Such approaches are important in addressing targeted issues in specific sectors or in regards to specific content. They are however limited in their ability to address the systemic, horizontal problems identified in the single market for digital services and would not address comprehensively the risks and due process challenges raised by today's online governance. Ultimately, this option was discarded for four main reasons: (i) the E-Commerce Directive is horizontal in nature and its revision requires a horizontal approach; (ii) the identified risks and problems are systemic and lead to cross-sectoral societal concerns; (iii) sector-specific legislation can lead to inconsistencies and uncertainties; and (iv) only horizontal rules ensure that all types of services and all categories of illegal content are covered.

170 Fundamental changes to the approach on the **liability regime for online intermediaries:** Annex 9 presents a series of considerations for different theoretical models of liability for intermediaries. The liability exemption of online intermediaries is a cornerstone for the fair balance of rights in the online world[111]. Any other model placing more legal risks on intermediaries would potentially lead to severe repercussions for citizens' freedom of expression online and traders' ability to conduct their businesses online and reach consumers. They would also be prohibitive for any new business, reinforcing the stronghold of very large players, able to sustain and, to a certain extent, externalize costs. Conversely, options significantly decreasing the standard for hosting services to quality for the liability exemption would severely affect the safety and trust in the online environment.

[111] The ECHR has indicated that it is "in line with the standards on international law" that ISSPs should not be held responsible for content emanating from third parties unless they failed to act expeditiously in removing or disabling access to it once they became aware of its illegality (see Tamiz v. the United Kingdom (dec.), no. 3877/14, 84, and Magyar Jeti, 67)

171 Changes to the **single market principle** set in the E-Commerce Directive and the requirement for the country of establishment to supervise services would inherently undermine the development of digital services in Europe, allowing only the very large players to scale across the single market. The single market principle is also the optimum model for ensuring that rules can effectively be enforced against services. The evaluation of the E-Commerce Directive and all other available evidence shows that that the single market principle has been instrumental for the development of digital services in Europe. This principle increased legal certainty and reduced compliance costs significantly, which is crucial for smaller services in particular.

172 Change to the prohibition on **general monitoring obligations**: the provision is core to the balance of fundamental rights in the online world. It ensures that Member States do not impose general obligations which could disproportionately limit users' freedom of expression and freedom to receive information, or could disproportionately burden service providers excessively, and thus unduly interfere with their freedom to conduct a business. It also limits online surveillance and has positive implications in the protection of personal data and privacy. Allowing such a disproportionate burden would likely lead to numerous erroneous removals and breaches of personal data, resulting in extensive litigation. Options for changes to general monitoring obligations were considered, and then discarded for non-compliance with the balance of rights described here.

173 Laying down **prescriptive rules on content which could potentially be harmful** to certain audiences, but which is not, in itself, illegal. The Impact Assessment focuses on illegal information and activities and on processes, tools and behaviours which might create or increase harms (i.e. recommender systems and other design choices for accelerating and selecting information flows). It is understood that content which is not illegal cannot be subject to the same removal obligations as illegal content.

174 Alternative options for the governance structure:

- **An expert group including Digital Services Coordinators**, managed by the Commission: this would at most ensure a limited, and less structured information sharing among national authorities.
- **Assigning the competences to an existing body**. Following an initial screening of the competences, capabilities and mission of the BEREC Office, ENISA, the Cybersecurity Competence Centre, EDPB, EDPS, Europol, no appropriate synergies were identified.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

175 The policy options were evaluated against the following economic and societal impacts, with a particular focus on impacts on fundamental rights.

Table 3 Summary of impacts for each option considered (compared to the baseline)

Impacts assessed	*Baseline*	*Option 1*	*Option 2*	*Option 3*
Economic impacts				
Functioning of the Internal Market and competition	~	+	++	+++
Costs and administrative burdens on digital services	~	>	>>	>>[112] / >>>[113]

[112] For all intermediaries, costs are equivalent with those in Option 2, apart from very large online platforms

Competitiveness, innovation, and investment	~	+	++	+++
Costs for public authorities	~	>	>>	>>>
Trade, third countries and international relations	~	+	+	+
Social impacts				
Online safety	~	+	++	+++
Enforcement and supervision by authorities	~	+	++	+++
Fundamental and rights (as laid down in the EU Charter)				
Freedom of expression (Art 11)	~	+	++	+++
Non-discrimination, equality, dignity (Art 21, 23,1)	~	+	++	+++
Private life and privacy of communications (Art 7)	~	+	+	++
Personal data protection (Article 8)	~	~	~	~
Rights of the child (Art 24)	~	+	++	+++
Right to property (Art 17)	~	+	+	+
Freedom to conduct a business (Art 16)	~	+	+	+
User redress	~	+	++	++
Overall	~	+	++	+++

6.1. Economic impacts

6.1.1. Functioning of the internal market and competition

176 All options considered would have an overall positive effect on the **functioning of the single market**, but there are notable differences between options. They all follow and build on the cornerstone of the single market for all digital services set in the E-Commerce Directive, and reinforce to varying extents the cooperation of national authorities in supervising the new obligations considered in each option.

177 The first option would in particular support the access to the single market for European Union platform service providers and their ability to scale-up by reducing costs related to the legal fragmentation rapidly escalating across Member States (as per section 6.1.2 below). It would also improve legal clarity and predictability by increasing transparency about content moderation measures and business users of online platforms through harmonized rules, as well as improve the cooperation between Member States in addressing cross-border issues.

178 The second and the third option would in addition further establish trust across Member States through an agile cooperation mechanism for cross-border concerns. This would add legal predictability for intermediary services active in several Member States. Importantly, it would also facilitate the effective enforcement of rules throughout the single market, where the Member State of establishment is most generally easily able to coerce a service provider, if need be, but other Member States would equally have an effective channel for making sure that the particular challenges of their state are appropriately addressed.

[113] Option 3 requires further obligations triggering higher costs than option 2 for a narrow population of very large online platforms; these are proportionate to the financial capacity of the very large companies generally captured by the scope of the definition.

179 In addition, the third option would couple the cooperation mechanism with an EU level body, allowing for fully coordinated actions and addressing in a consistent and more efficient way issues common to several Member States. Both sub-options address this and provide for different mechanisms for ensuring an EU level enforcement or rules when very large platforms are concerned, ensuring maximum consistency across the single market.

180 In a model reflecting only the concerns related to legal fragmentation, addressed in all three options, the legal harmonisation of obligations across the single market should lead to an **increase of cross-border digital trade of 1 to 1.8%**[114]**.** This is estimated to be the equivalent of an increase in turnover generated cross-border of EUR 8.6 billion and up to EUR 15.5 billion[115].

181 With regard to effects on **competition**, all three options are proportionate and do not impose dissuasive requirements for service providers. By harmonising the legal requirements across Member States, they all establish a level playing field for emerging services across the single market. The third option would establish asymmetric obligations on very large online platforms with a systemic impact in Europe, making sure that smaller, emerging competitors are not affected by disproportionate obligations, while ensuring that certain systemic policy concerns are adequately addressed by very large online platforms. The asymmetric obligations would lead to higher costs for approximately 20 of the largest platforms in the EU and the world, both in terms of users reached and turnover. These enhanced obligations are necessary to secure online safety and fight against illegal activities efficiently. They would also lead to significant improvements of the service itself, not least in enduring a safer environment for their users and the respect of their fundamental rights; in turn, this will likely benefit the platform itself when compliant with the requirements. However, smaller companies could also take similar measures on a voluntary basis, and would be invited to be part of the co-regulatory framework (e.g. on content moderation and crisis management, on advertising transparency).

6.1.2. Competitiveness, innovation and investment

182 With the additional legal certainty, all three options are expected to have a positive **impact on competitiveness, innovation and investment in digital services**, in particular European Union start-ups and scale-ups proposing platform business models but also, to varying extents, on sectors underpinned and amplified by digital commerce. The legal certainty provided by the intervention would likely encourage investments in European Union companies.

183 The first option would primarily affect online intermediaries established in Europe by **cutting the costs** of the evolving legal fragmentation and allowing services to repurpose resources in growing their business and, potentially, investing in innovative solutions. It would in addition create a true regulatory **level playing field** between European Union-based companies and those targeting the single market without being established in the EU.

[114] See Annex 4

[115] Using as benchmark private sector estimates of online cross-border trade https://www.cbcommerce.eu/press-releases/press-release-cross-border-commerce-europe-publishes-the-second-edition-of-the-top-500-cross-border-retail-europe-an-annual-ranking-of-the-best-500-european-cross-border-online-shops/

184 The second and third options would bring stronger improvements to the cooperation mechanisms across Member States and harmonise a wider spectrum of provisions, including transparency requirements in online advertising. They would thus affect a wider spectrum of digital services and limit current and emerging costs of legal fragmentation, compared to the first option and the baseline scenario.

185 Further, all three options would preserve the equilibrium set through the conditional liability exemption for online intermediaries, ensuring that online platforms are not disproportionately incentivised to adopt a risk-averse strategy and impose too restrictive measures against their business users (and citizens using their services). This is particularly sensitive in the recovery phase of the COVID-19 crisis, where sectors such as tourism, accommodation, food and transport require predictability and a reinforcement of their online presence.

186 Overall, the three options will lead to better conditions for the underlying digital services will result in more choice for both businesses and consumers. This will cascade into increase in e-commerce, in particular cross-border[116], including positive impacts on the creative industry, manufacturing, information service and software, etc. Consequently, all three options will have a positive effect on **the competitiveness of legitimate business users** of online platforms, manufacturers or brand owners, by reducing the availability of illegal offerings such as illegal products or services (and, of course, reducing harms on consumers, as per 6.2.1 below). In addition, the legally guaranteed availability of the internal and external complaint and redress mechanisms would afford other better protections against erroneous removal and limit losses for legitimate businesses and entrepreneurs.

187 The **macroeconomic expected impact** of Option 1, once fully implemented, amounts to an increase of 0.3% of GDP benchmarked against 2019 values – i.e. a total of EUR 38.6 billion.[117]

188 Options 2 and 3 would reach better results by removing disincentives for platforms established in the Union to take appropriate voluntary measures, in both ensuring a higher scale of illegal activities and information online, and in safeguarding users' rights. The **macroeconomic impacts** of Option 2 are estimated at a 0.4 increase of GDP (EUR 61.8 billion)[118].

189 Option 3 would produce better results than option 2, in applying asymmetric obligations to the largest online platforms where a large share of the economic loss occurs. A risk management approach would address in a targeted manner areas of abuse and systemic failures. It would in addition afford enhanced transparency on key processes related to the prioritisation of information which reaches consumers through online advertising and recommender systems. This would build further resilience into the system, giving more choice and agency to users and stimulating an innovative and competitive environment online. The **macroeconomic impacts** of Option 3 are estimated at a 0.6% increase of GDP (EUR 81.7 billion). An alternative model[119] following a different methodology estimates a EUR 76 billion increase in EU GDP over the 2020-2030 period for a package of measures broadly equivalent to Option 3.

[116] *Supra,* §180
[117] See Annex 4
[118] *Ibidem*
[119] Niombo Lomba, Tatjana Evas, *Digital Services Act. European added value assessment*, European Parliamentary Research Service, October 2020

6.1.3. Costs and administrative burdens on digital services

190 All three options incur costs for online intermediaries. However, these costs represent a significant reduction compared to those incurred under the present and evolving fragmented and uncertain corpus of rules.

191 **At company level**, in a simple model quantifying only the harmonising rules common to all three options, the legal intervention would already close the Single Market gap with a cost reduction of around EUR 400.000 per annum for a medium enterprise assumed present in three Member States. Compared to projected scenarios where the legal fragmentation would become more acute, the intervention would lead to savings of EUR 4 million for the same scale of company present in 10 Member States and EUR 11 million for an extreme scenario of fragmented rules in each of the 27 Member States of the Union. The cost savings are most impactful for micro- and small- enterprises, where the current fragmentation is prohibitive for offering services in more than two Member States.[120]

192 Direct costs for the main due diligence obligations are common across all three options and depend to a large extent on the number of notices and counter-notices received by a platform and cases escalated to an out of court alternative dispute resolution system. Estimates are considered based on an initial scale of notices received, but can vary to a large extent.

193 For **out of court alternative dispute resolution systems,** there is a level of uncertainty, as no reliable data or precedent allows to estimate what volumes of complaints would be escalated. The existence of alternative dispute resolution mechanisms in all Member States would however facilitate access to such mechanisms and likely append negligible costs compared to the current system.

194 In addition to these costs, for the second option, services would also incur some technical design, maintenance and reporting costs, for the additional information and transparency obligations presented in paragraph 156. However, these are expected to be marginal and absorbed into the general operations and design costs of online platforms and ad intermediaries, respectively. As these measures are intimately related to the type of service offered and design choices of the service itself (e.g. development and use of recommender systems, ad intermediation, marketplaces intermediating services and sale of goods), micro-enterprises would not be exempted from scope.

195 In option 2, costs related to information requirements would equally be reduced rather than increased, compared to the baseline, by streamlining and harmonising the requirements, thereby preventing further legal fragmentation and possible compliance requirements with very divergent national systems.

196 In addition, the third option includes a series of potentially significant costs which are limited to very large online platforms. First, the enhanced transparency and reporting obligations for content moderation, recommender systems and online advertising would bring technical and maintenance costs which would be absorbed in the services' operations. A fixed cost for the organisation of risk assessments and annual audits would also be incurred by very large platforms. Risk mitigation measures will, however, vary to a large extent depending on the initial design of the systems, and the severity of risks. Overall the additional costs for such service providers range from EUR 300.000 to EUR

[120] See Annex 4

3.500.000 *per annum* for the additional obligations, excluding potential variable costs for risk mitigation measures.

197 The table below presents an overview of the cost estimates at company level for each option.

Table 4 Estimates of costs at company level[121]

Type of obligation	Option 1	Option 2	Option 3
1. *Notice and action obligations and information to users, absorbing complaints and redress costs*	<u>For all hosting service providers:</u> Highly dependent on the volume of notices received, where personnel costs are the most notable expenditures. Estimates range from a one-off maximum cost of EUR 15.000 for establishing a notice-and-action technical system and light maintenance, to EUR 1 million for a volume of 200 notices received per day, and EUR million for 3000 notices received per day. While there are some economies of scale with the increase of the number of notices, these are limited. These are indicative costs and, for most companies, they do not represent an additional cost compared to current operations, but require a process adaptation in the receipt and processing of notices and streamline costs stemming from fragmented obligations currently applicable.		
2. *Legal representative*	<u>For some online intermediary services not established in the EU and with a significant user base in the EU:</u> Estimated between EUR 50.000 to EUR 550.000 per annum, depending on the FTE necessary to complete the tasks. These costs can be partially or fully absorbed, for most companies, in existing requirements for legal representatives.		
3. *Transparency reporting*	<u>For all intermediary services (exempting small and micro-enterprises):</u> 0.1 and up to 2 FTEs and one-off development data collection, absorbed in the development of systems		
4. *User-facing transparency of advertising and recommender systems*	\	<u>Online platforms (exempting small and micro enterprises)</u> Costs absorbed in the routine development of systems Data collection and availability as regards information on the functioning and targeting criteria, when applicable, by and large absorbed into GDPR compliance, with minor additional costs for up-front information publication	
5. *Risk management obligations*	\	\	<u>Very large platforms:</u> Risk assessments: estimated between EUR 40.000 and EUR 86.000 per annum Audits: between EUR 55.000 and 545.000 EUR per annum Risk mitigation measures are variable costs and can range from virtually no costs, to significant amounts, in particular when the platforms' systems are themselves causing and exacerbating severe negative impacts. The duration and level of expenditure for such measures will also vary in time. Similarly, participation in Codes of conduct and crisis protocols requires attendance of regular meetings, as a direct cost, but the streamlined targeted

[121] Cost models and benchmarks presented in Annex 4

			measures can vary.
6. Ad archives	\	\	Very large platforms (that run advertisements on their platforms): Up to 220.000 EUR for building APIs to give access to data and quality controls for data completeness, accuracy and integrity, and for system security and availability.
7. Compliance officer	\	\	Very large platforms Estimated between 1-5FTEs

SME test

198 For a micro-enterprise, the costs of the legal fragmentation seem prohibitive today: the modelled costs when providing services cross-border are higher than the maximum annual turnover of a micro-enterprise when offering services in several Member States. The harmonised rules under all options would cut duplication costs for SMEs as well as costs from legal risks with regards to the harmonised provisions for each option.

199 With regard to SMEs offering platform services, since they do not reach a scale in their user base equivalent to that of very large online platforms, the illegal activities conducted by their users would not reach a similar impact. There are exceptions to this. First, the user base of successful online platforms typically scales very fast; second, even the smaller services can be instrumental to the spread of certain crimes online. On some occasions[122], microenterprises can be aggressively targeted by perpetrators, not only leading to societal harm, but also corrupting the legitimate value proposition of the digital service. Consequently, SMEs cannot be fully exempted from the minimum requirements for establishing and maintaining a notice and action mechanism under each of the options.

200 Costs of the notice and action system are proportionate to the risks posed by each service: an average micro-enterprise receiving a volume of 50 notices per annum, out of which 5% would make the object of a counter-notice procedure, should sustain a cost of approximately EUR 15 000 per annum. The introduction of standard, minimum requirements for notices, procedures and conditions, as well as reporting templates, should further decrease the expected costs for small companies, supporting them in tackling illegal content and increasing in turn the legal certainty.

201 Should the volume of notices increase exponentially, this would likely correspond to a generalised exploitation of the service for illegal activities. The costs for processing the notices could become prohibitive, but, conversely, a non-responsive service would likely bear legal consequences even under the baseline scenario, and would lose its legitimate

[122] Such as requests for help from microenterprises in the context of the EU Internet Forum, where their services were targeted by terrorist organisations to pivot the dissemination of content by sharing hyperlinks on their services.

users. A notice-and-action system can be a powerful support for legitimate businesses who intend to address illegal activities carried out by their users.

202 Under all options, the additional transparency obligations are expected to be proportionate to the risks and capacity of each service provider and should be absorbed in the operations and design of the systems. However, these costs could be in themselves disproportionate for a small or micro-enterprise and the risks such companies pose, and the impacts they may have do not justify such limitations on the companies.

203 Option 3 specifically includes targeted obligations for very large platforms. These are not expected to be SMEs under any circumstance, as both the number of employees and the global turnover of such platforms is significantly higher than those of a medium-sized enterprise. However, thresholds for 'very large platforms' would be set proportionately to their reach in terms of number of users in the Union, but would not exempt SMEs by virtue of the risks and societal harms such services could cause.

6.1.4. Costs for public authorities

204 The supervision and enforcement of the rules would be key in ensuring the success of the intervention. An appropriate level of technical capability within public authorities, robustly built over time, will ensure a correction of information asymmetries between authorities and digital services and the relevance of the public intervention in a sustainable model of online governance. From this perspective, any additional measures to mutualise resources and expertise, and establish sound IT infrastructures for cooperation can have a net positive effect in assisting all Member States in the medium- to long-term.

205 Compared to the baseline, each of the three options should significantly cut the costs brought by the inefficiencies and duplication in the existing set-up for the cooperation of authorities (see driver 2.3.6). With regard to law enforcement, a smoother, more reliable cooperation with digital services, not least in processing requests, would improve the effectiveness and efficiency of their actions. Net cost reductions, however, may not be expected, since the volume of illegal activities online is far larger than the capacity of law enforcement authorities to investigate these offences.

206 With the first option, national authorities would follow a clear, streamlined process for cross-border issues, with clear resolution and response. Member States where a large number of services are established are likely to need some reinforcements of capabilities. These will be attenuated, however, through the creation and use of a clearing house system for cooperation across authorities, including technical costs for the development and maintenance (by the Commission), as well as running costs for the Member States' appointed authorities to engage in the cooperation, either to issue or to respond to requests. Information flows and data collected through the clearing house should significantly improve the ability of Member States to supervise the systemic compliance of services with the requirements.

207 For the second option, a digital coordinator would need to be appointed in each Member State, interfacing with the other EU authorities and assuming a coordination role among the competent authorities in their country. While the coordinator would require some costs, the efficiency gains are expected to outweigh them in every Member State: efficiency gains for the individual authorities through mutualisation of resources, better information flows, and straight-forward processes for interacting with their counterparts across the single market, as well as with service providers.

208 For the third option, an additional cost would be born at EU level, creating further efficiency gains in the cooperation across Member States and mutualising some resources for technical assistance at EU level, for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.

Table 5 Summary of costs for authorities for each option considered

Type of activity	*Option 1*	*Option 2*	*Option 3*
1. Supervising systemic compliance with due diligence obligations for all services (country of establishment)	*Cost efficiencies:* streamline evidence and information for supervising platforms through the clearing house system. *Direct costs:* varying from 0.5 FTEs up to 25 FTEs, depending on scale of services hosted[123]		
2. Supervision of enhanced obligations for online platforms – expenditures at MS level	\	\	*Significant cost efficiencies* through enhanced transparency obligations on platforms Costs expected to fluctuate depending on inspections launched. For one inspection/audit, estimates between EUR 50.000 and EUR 300.000.[124] Codes of conduct and co-regulatory framework: investment at EU level of 0.5-2 FTEs per initiative – absorbed in costs in section 3 below
3. Supervision and governance at EU level	\	\	Sub-option 3.A: - European Commission : 50 FTEs + EUR 25 mil operational budget - Member States : 0.5 - 1 FTE for participation in the Board Sub-option 3.B: - EU Board decentralised agency 55 FTEs (operations and admin) + EUR 20 mil operational budget - European Commission: 10 FTEs + EUR 10 mil. operational budget Member States : 0.5 - 1 FTE for participation in the Board - Member States : 0.5 - 1 FTE for participation in the Board
4. EU-level: for clearing house and coordination	*Significant cost efficiencies* expected from smoother, clearer cooperation processes One-off: 2 mil per annum over the first two years for technical development. Maintenance and additional development over the next 3 years of approx. EUR 500.000 in total		

[123] Benchmarked against resources currently reported by DPAs, and estimating 0.5 FTE for investigators per 15 million users reached by a digital service hosted in the Member State, with efficiencies of scale accounted for

[124] (LNE, forthcoming)

5. *Law enforcement actions & public authorities requests (re. supervision of illegal activities online)*	*Cost efficiencies:* streamline cooperation processes for cross-border assistance; clear process for information requests to digital services and information obligations *Direct costs:* no direct costs entailed by the measures, but no net reduction of costs expected, as volumes of illegal activities consistently higher than law enforcement capacities

6.1.5. Trade, third countries and international relations

209 All three options are expected to have an impact in **diminishing illegal trade into the Union**, both in relation to direct sellers and sellers intermediated by online platforms.

210 All options would require a legal representative in the Union and extend the scope of the due diligence obligations to service providers established outside the EU thereby ensuring EU users' rights are protected in the global online space. This is not expected to have a significant effect on **legitimate platforms from third countries targeting the single market,** with further proportionality incorporated by excluding very small, incidental providers. For most platforms, it is likely that legal representatives are already established as part of other legal requirements under EU legislation (e.g. General Data Protection Regulation[125] ('GDPR'), which would absorb to a large extent this cost. In addition, compliance with EU rules could be a commercially beneficial trust signal for such providers.

211 The intervention would inherently set a **European Union standard in the governance of issues emerging on online platforms**, both in relation to measures to mitigate risks and ensure online safety, and the protection of fundamental rights in the evolving online space. Most international fora, including the G7 and the G20, but also international organisations such as the UN, the OECD and the Council of Europe have flagged such concerns, and other jurisdictions have taken measures or are currently discussing taking measures – including amongst others the US, Australia, Canada, India, New Zealand. Action in this field by the European Union will lead to enhanced cooperation and engagement with third countries in this context.

212 The first option, more limited in the scope of measures, would still set a regulatory standard in particular on the due process and information requirements from platforms, encouraging a fundamental rights-centric approach. The second option would in addition firmly clarify the balance of rights set through the liability regime for online intermediaries, a controversial and politicised topic in some other jurisdictions, and would set a higher standard of transparency and accountability for online platforms. The third option would place the European Union in a leadership role, not least through establishing an EU-level body supporting the oversight of the largest, most impactful platforms, and establishing an important capability for auditing and investigating such platforms in a flexible manner, in anticipation of emerging risks.

213 From an international trade perspective, the provisions are in line with the non-discrimination provisions in the GATS, as they follow objective and non-discriminatory criteria, regardless of the location of the headquarters or the country where the company historically originated. This is also the case in establishing whether, in option 3, service

[125] 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

providers fall into the category of 'very large online platforms' as the scope is defined exclusively by the objective metric of number of users.

6.2. Social impacts

6.2.1. Online safety

214 As a primary objective for the intervention, all three options contribute to an appropriate governance for ensuring online safety and the protection of consumers from illegal offerings.

215 All options would significantly improve the baseline, making sure that **all types of illegal content, goods and services** can be flagged in a harmonised manner across the Union. This would ensure a coherent horizontal framework instead of the currently inconsistent approaches relying on the private policies set by online platforms or the regulatory and self-regulatory efforts in Member States or at EU level. It would also ensure that **cooperation with law enforcement, national authorities and other trusted flaggers** is appropriately accelerated, improving the ability of authorities to tackle cybercrimes and other online crimes. In certain cases, this would lead to positive effects on their ability to protect the right to life and security of individuals.

216 The second and the third option would also stimulate online platforms to take **additional measures**, proportionate to their capability, adapted to the issues and illegal content they most likely host, and in full respect of fundamental rights. 12%[126] of the service providers responding to the open public consultation reported that they used automated systems for detecting illegal content they host, and the same percentage had policies against repeat offenders on their platform. Voluntary measures for tackling illegal content have proven effectiveness at scale. At the same time, such measures continue to be prone to errors, both in under- and over- identifying content. The two options do not only provide for legal clarity for service provider to enforce their measures, but they also establish a missing due process around such processes. The two options set stronger safeguards through transparency and accountability, when private companies take such detection measures. The third option would in addition ensure a higher level of supervision of the effectiveness as well as the pitfalls and errors in the content moderation put in place by platforms, with a particular focus on very large platforms.

217 The second and the third options would also tackle **systemic risks** posed by online platforms through the way they prioritise and accelerate the distribution of content and information. They would both correct information asymmetries and empower citizens, businesses and other organisations to have more agency in the way they interact with the environment and information intermediates by platforms. This would also put consumers in a better informed position for making choices, be it in buying goods and contracting services, or simply in consuming information online.

218 The third option, however, would include a much stronger accountability mechanism taking into account the disproportionate influence of very large platforms specifically, ensuring access to researchers and appropriately resourced competent authorities to relevant information allowing them to assess the platforms measures taken in co-regulatory processes to address the risks.

[126] Out of 362 service providers

219 As the COVID-19 crisis and incidents of viral spread of illegal content have shown, **crisis situations** can manifest online, presenting systemic risks on platforms which reach millions and requiring coordinated interventions. The third option would also include a framework for establishing such cooperation in crisis situations through setting up crisis protocols, together with the appropriate checks and balances for both platforms and authorities.

6.2.2. Enforcement and supervision by authorities

220 A first notable impact, already explained in section 6.2.1, is the improved ability of law enforcement and authorities to **supervise and tackle online crimes**.

221 In addition, all three options entail an important impact and capital improvement as compared to the baseline, in establishing the competence for authorities to supervise not only the incidence of illegal activities online and systematic failure to respond to notices, but also the performance of the notice and action and broader moderation systems in **protecting users and avoiding over-removal of legal content**. They would all allow designated authorities to request appropriate interim measures, where failures are observed, and eventually apply proportionate and dissuasive sanctions for systematic non-compliance with the due diligence obligations. Ultimately, where all other means fail and where there are severe consequences from the systematic non-compliance, implying the threat of life and security of persons, and following the decision of a court, blocking measures can be applied. The broad spectrum of measures will allow authorities to effectively supervise and enforce the rules, and would remain proportionate by applying gradually and allowing the service provider to take corrective measures to cease the infringement and, under any circumstance, make use of established appeal mechanisms. The reinforced coordination through the national Digital Coordinators in option 2, and the EU competence in option 3, would each significantly increase the coherence and capacity of authorities to supervise and calibrate the imposed measures.

222 Importantly, the second and the third option each harmonise conditions for court and administrative orders requesting removal of content. This should facilitate the actions of the authorities and lead to better enforcement overall. In addition, option 3 further facilitates the ability of national authorities to supervise services (such as accommodation or transport services) offered through the intermediation of online platforms.

223 The second option gives more agency to users through more robust transparency tools, and the third option sets the highest standard of supervision for all content moderation mechanisms, as well as online advertising and recommender systems.

6.3. Impacts on fundamental rights

224 The protection of fundamental rights is one of the main concerns in the online environment, marked by the complexity of interests at stake and the need to maintain a fair balance in mitigating risks. This assessment played a core part in the consideration of the wider range of options and determined the discarding of several options.[127]

225 All three of the retained options are generally well balanced and are not expected to have a negative impact on fundamental rights. The main differences between the options are rather linked to the extent of their effectiveness in safeguarding fundamental rights and

[127] See, for options on liability of online intermediaries in Annex 9, and for the use of proactive detection measures, supported by technical tools and automated decision systems, Annex 11

their ability to continue to offer a 'future proof' due process faced with the evolving risks emerging in a highly dynamic digital environment.

226 All three options would also include a requirement to companies to adopt a fundamental rights standard when implementing the due diligence obligations set by the intervention. This would require services to assess and manage risks in a proportionate and appropriate manner.

227 Where option 3 requires a regular risks assessment from very large online platforms, this equally includes an assessment of the way the platforms' systems or use affect the protection of fundamental rights such as freedom of expression, right to private life, non-discrimination or rights of the child. Consequently, they have to adapt the design of their systems and take appropriate measures to address significant risks, without prejudice to their business freedoms. Further, in the design of codes of conduct and crisis protocols under this option, such requirements will continue to apply, and appropriate checks and balances are to be set up, notably through reporting and transparency commitments from all participants, including authorities involved, participation and scrutiny from civil society and academia, and, finally supervision by the EU board and national authorities.

228 The fundamental rights most clearly touched upon by the intervention are the following:

6.3.1. Freedom of expression (Art 11 EU Charter of Fundamental Rights)

229 Content moderation decisions by private companies, be it in assessing legality or compliance with their own terms of reference, can impede freedom of expression, in terms of freedom to share information and to hold opinions, but also in terms of freedom for citizens to receive information. While the sale of goods might be seen as less related to freedom of expression, speech can also be reflected in goods, such as books, clothing items or symbols, and restrictive measures on the sale of such artefacts can affect freedom of expression. In this context it is important to underline that all three options will only require removal of content that is illegal. Nevertheless, the options also address the need to provide safeguards in the form of complaint systems and transparency requirements that will mitigate negative consequences of services' removal of content based on their own terms of service.

230 None of the options include prior authorisation schemes, and they all prohibit Member States from establishing such requirements for digital services. Such measures can amount to a severe limitation of freedom of expression.

a. Mitigating risks of erroneously blocking speech

231 All three options would add substantial improvements to the baseline situation, by imposing mandatory safeguards when users' content is removed, including information to the user, complaint mechanism supported by the platform, external dispute resolution mechanism. Coupled with transparency reporting and oversight for systematic compliance by authorities, these are key elements for ensuring the safeguards missing in the baseline and ensuring that users' rights are respected and they are empowered to defend themselves against erroneous sanctions and removals of their content.

232 The Court of Justice has repeatedly confirmed that requirements for platforms to deploy automated content moderation 'could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful

communication'[128]. At the same time, service providers use such tools, not least for enforcing their terms of service, with improving levels of accuracy, but also with significant challenges, including but not limited to the inability of such tools to accurately distinguish context-dependent content.[129]

233 None of the option would require the deployment of such tools. Instead, all three options would preserve the prohibition of general monitoring obligations and would, in addition to the baseline, reinforce safeguards for users to seek redress following removals. Importantly, the second and the third option would extend these obligations to services established outside of the Union but targeting the single market.

234 The second and the third option would also remove disincentives for European platforms to take measures for tackling illegal content, goods or services shared by their users by clarifying that this does not, in itself, place them outside of the liability exemption for intermediaries; such measures could include the use of automated tools.

235 The third option would include an additional important safeguard where very large online platforms are concerned (and where impacts of removals are most severe on users' rights): it would impose enhanced transparency and reporting obligations on process and outcomes of content moderation, including automated tools, and afford competent authorities with inspection and auditing powers, opening systems for scrutiny also by researchers and experts. It would also include explicitly as part of the mandatory risk mitigation obligations considerations for their users' freedom of expression, including concerning the way the very large platforms design and maintain their systems. This includes, for example, the design of their recommender systems, but also of the content moderation systems and tools. This would set the highest standard of protection and accountability and maintain a flexible and vigilant possibility to detect and mitigate risks as they emerge.

b. Addressing other chilling effects on speech

236 Some evidence shows that highly violent online environments, for example, can have a chilling effect on speech, for instance where there is a proliferation of illegal hate speech or other forms of illegal content. Such chilling effect has been reported to e.g. risk influencing individuals' rights to political participation[130]. All options would empower users to report illegal content and support a safer online environment (see section 6.2.1 above).

c. Stimulating freedom to receive information and hold opinions

237 All three options would affect the freedom to receive information by ensuring that legal content, of general interest to users, is not inadvertently removed, as explained in paragraphs 231 to 233 above. In fostering exchanges of information, this can also have spill-overs on users' freedom of assembly and association.

238 In addition, the second option would further empower users to better understand and control their online environment through transparency measures concerning recommender systems and online advertising. This is particularly important in allowing citizens to participate in democratic processes or empowering consumers to make informed choices. The third option would establish a higher standard of accountability

[128] Cases C-70/10 (SABAM v Scarlet) and C 360/10 (SABAM v Netlog NV)
[129] See Annex 11
[130] United Nations Special Rapporteur on violence against women, thematic report on violence against women in politics: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/73/301.

for those platforms fostering a 'public space' for speech and commercial exchanges, by imposing asymmetric obligations for transparency and oversight of such systems, and providing for a more impactful and targeted effect.

6.3.2. User redress

239 The three options would have a fundamental impact on users' possibilities to challenge decisions by platforms, both in what concerns citizens, and businesses. This is one of the biggest impacts of the intervention, compared to the baseline, ensuring a fair governance and empowering users to exert their rights.

240 All three options include a **complaint and redress mechanism**, staged in two steps: obligation to offer and process such complaint by the service provider and availability of out of court dispute settlement mechanisms, expected to absorb escalated issues and to resolve them in a faster and less resource intensive manner than court proceedings. Users would always be able to appeal to the court system, in accordance with the applicable rules of national law.

241 The enhanced **transparency provisions**, making users aware of the policy applied to hosted content, goods or services, as well as the specific information to the user, once corrective action is taken against them, are *sine qua non* conditions for an effective remedy. All three options would ensure such a standard and would also sanction systematic failure from service providers to provide redress mechanisms. In addition, where the third option affords enhanced supervisory powers for authorities regarding very large online platforms, where users' rights can be most severely affected, this additionally supports users' right to remedy.

242 Finally, in what concerns **restrictions potentially imposed by authorities**, the established judicial remedy options would always be available to service providers, as well as to platforms' users whose content/goods/services are subject to such requests. The enhanced cooperation mechanism across authorities, set up in option 2 and, to a larger extent, in option 3 would further strengthen the checks and balances and the availability of redress in this regard.

6.3.3. Non-discrimination (Art 21 of the Charter), equality between women and men (Art 23) and the right to human dignity (Art 1)

243 All three options would have a positive impact in mitigating risks for persons in vulnerable situations and vulnerable groups to be exposed to discriminatory behaviours and would protect the right to human dignity of all users of online services. This concerns first a **disproportionately unsafe online environment**. In this regard, each option would have different strengths of impact, as assessed in section 6.2.1 above.

244 Second, such groups or individuals could be overly affected by restrictions and removal measures following from biases potentially embedded in the notification system by users and third parties, as well as replicated in automated content moderation tools used by platforms. In addition, to the extent that the second and the third option also include a clarification of the liability exemptions with regard to voluntary measures taken by service providers to tackle illegal activities, it is possible that more service providers would voluntarily engage in content moderation. Currently, in particular for large online platforms, such voluntary measures also include the use of content detection technologies, algorithms predicting abusive user accounts or other filtering technologies. Each of these technologies and the way they are designed, trained, deployed and

supervised in specific cases, present different risks for non-discrimination and gender equality, but also to the protection of personal data and privacy of communications.

245 The three options would address the risks by affording **safeguards aimed at improving the possibility for contesting such restrictions** (as per 6.3.2). In addition, the third option offers enhanced inspection powers to national authorities for the content moderation processes of very large platforms, where the impact of discriminatory practices can be most acute.

246 The second and the third option would cater for **broader discrimination concerns** emerging in the way platforms amplify information, and access to goods and services: they would include transparency provisions for recommender systems and placement of online ads, empowering users to understand and have agency over how they are affected by these systems.

247 The enhanced transparency and oversight measures included in the third option for content moderation, recommender systems and online advertising through very large online platforms would be particularly impactful in offering the means for detecting discriminatory practices and allowing these issues to surface on the policy and public agenda.

6.3.4. Private life and privacy of communications (Art 7 of the Charter) and personal data protection (Article 8 of the Charter)

248 Nothing in the intervention should prejudice the high standard of personal data protection and protection of privacy of communications and private life set in EU legislation. All measures following from either one of the three options should be fully compliant and aligned.

249 Furthermore, all measures are aimed to enhance users' online safety and can be expected to contribute to better responding to illegal content and activities, including content consisting of the non-consensual sharing of users' private data, including images.

250 For all three options, obligations to set up a **'Know Your Business Customer'** policy and collect identification information from traders, as well as obligations to for the identification of advertisers would likely imply processing and disclosure of personal data. However, these measures are limited to traders, and do not concern other users of online platforms. With regard to the data requested for traders under the 'know your business customer' obligations, the requirements are limited to the minimum necessary, as established in other similar regulatory initiatives[131] and best practices in industry[132].

251 Similarly, where option 3 requires further reporting to national authorities, this can entail disclosure of personal data of users of platforms (e.g. accommodation service providers, sellers of goods). This is a necessary measure for protecting the public interest and the protection of consumers online, and remains proportionate by limiting the requirement to data already collected by the platform. It does not cover in any way requirements for citizens using online services to identify themselves. If personal data is part of the request, the requirement would offer a legal basis for data processing by the service provider in line with Article 6 (1) c) of the GDPR and would require Member States to

[131] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

[132] (European Commission, 2020)

specify the conditions for data processing by the requesting authorities, in the national laws laying the competence for such authorities to issue requests.

252 Where option 3 requires from large online platforms to **facilitate data access for audits and investigations by researchers,** such measures should be designed based on an appropriate assessment of risks, in line with GDPR requirements, potentially with the involvement of Data Protection Authorities, and should be organised with the least invasive approach and proportionate costs, exploring options for secure access or protected access.

253 Where option 3 requires service providers to notify to authorities suspicions of serious criminal offences, this is proportionate and justified by the seriousness of the offence and the public interest entailed. At the same time, the provision does not, in itself provide for a legal basis to process personal data of users of the platform, with a view of possible identification of criminal offences.

254 **Transparency and disclosure requirements** included in option 2, as well as requirements regarding the maintenance of **ad archives** in option 3 are not intended to lead to any additional or disclosing of personal data of the users who had seen the ads; they might include personal data of the advertiser, acting as a trader, and personal data already publicly disclosed in the content of the ad.

255 As regards risks posed by **automated content moderation and other technologies** voluntarily used by platforms for tackling illegal behaviours of their users – see paragraph 244 above – it is understood that a case by case assessment is necessary and, when service providers develop and deploy such tools, they must do so in observance of the rights and obligations established in the GDPR and the ePrivacy Directive[133]. None of the three options would affect in any way this requirement and they do not mandate the use of any automated tool for detection of content. Option 3 would instead potentially create additional opportunities for inspecting compliance in this regard. It also includes considerations for the right to private life in the risk assessment framework very large platforms are subject to.

256 All options include obligations for redress and complaint mechanisms; they imply that the content removed should be preserved by the service provider for the reasonable duration of such potential proceedings, allowing them, where necessary, to reinstate the content. Such measures have the sole purpose of enabling a 'due process' approach following a removal decision and are proportionate to the rights and interests of the content provider, data subjects whose personal data might be retained, and the service provider, which incurs very limited costs for the storage of data for a limited period of time.

6.3.5. Rights of the child (Art 24 of the Charter)

257 All three options would have a positive influence in protecting the safety of children online. Consistent, with the analysis in section 6.2.1 the positive impact is strengthened with each option. Option 3 explicitly includes rights of the child as a primary consideration when very large platforms assess the systemic risks posed by the design of their service and take appropriate measures to uphold the best interest of children.

[133] 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

6.3.6. Right to property (Art 17 of the Charter) and freedom to conduct a business (Art 16)

258 All three options would have a similarly positive impact on the right to property by complementing existing rules addressing the violation of intellectual property.

259 None of the measures in either one of the options should jeopardise the protection of trade secrets or proprietary products of online platforms. Where, in option 3, further requests for disclosure could be made by authorities to very large online platforms, these would entail a secrecy obligation on the public authority with regards to trade secrets.

260 All the three options will imply compliance costs and adjustments of the business processes to regulatory standards for the platforms. This limitation to the right to freedom to conduct a business is proportionate and will be mitigated and most likely be fully compensated by the fact that the measures will lead to significant cost savings compared to the baseline, in particular in light of the evolving legal fragmentation. Costs are also tailored to be proportionate to the capacity of the given service provider.

6.4. Environmental impacts

261 Environmental impacts are expected to be relatively marginal for all options compared to the baseline. This is not to say that the environmental impact of digital services will not be important to monitor. Substantial factors will depend on technological evolution, business choices in manufacturing and development chains, consumer behaviour and nudging, etc.

262 Digital services are not only energy consumers themselves and generators of digital waste, but are also underpinning services and distribution of goods which have themselves an important environmental footprint – including transport, travel and accommodation, etc. However, the three options are primarily expected to shift the focus towards responsible digital services, with a marginal impact on the overall demand of digital services. This makes it difficult to estimate with sufficient intervals of confidence a causality between the adoption of either three of the policy options and the environmental impacts of digital services.

263 In addition, many illegal activities are also related to intense polluting – see, in particular, the case of counterfeit products[134] or the manufacturing of dangerous products or the sale of products that do not comply with EU environmental or energy-saving rules (e.g. eco-design, energy labelling, etc.). A reduction in the ability to place on the European market such products might also reduce in their production. The due diligence obligations would also equally concern non-compliance with the extended responsibility requirements in online sales[135].

7. HOW DO THE OPTIONS COMPARE?

7.1. Criteria for comparison

264 The following criteria are used in assessing how the three options would potentially perform, compared to the baseline:

- **Effectiveness in achieving the specific objectives**:

[134] (European Commission, 2020)
[135] Waste Framework Directive 2008/98/EC

i. Ensure the best conditions for innovative cross-border digital services to develop
ii. Maintain a safe online environment, with responsible and accountable behaviour from online intermediaries
iii. Empower users and protect fundamental rights online, and freedom of expression in particular
iv. Establish the appropriate supervision of digital services and cooperation between authorities

- **Efficiency:** cost-benefits ration of each policy options in achieving the specific objectives
- **Coherence with other policy objectives and initiatives**:
  a. Within the Digital Services Act Package, coherence with the second initiative
  b. Other, sector-specific instruments, such as the AVMSD, the DSM Copyright Directive, the proposed Regulation on terrorist content
  c. Coherence with Internet principles and the technical infrastructure of the internet[136]
- **Proportionality:** whether the options go beyond what is a necessary intervention at EU level in achieving the objectives

7.2. Summary of the comparison

265 **Summary of the comparison** of options against the four criteria is included below. The table visualising the comparison of options should only be read in vertical, '+' pointing to a better performance of the option than the baseline, and '++++' to the best performance among the options; the '>' symbol is used to indicate higher costs than the baseline, and '>>>>' the highest cost among the options.

Table 6 Comparison of options

	Effectiveness	Efficiency		Coherence		
		Costs	*Benefits*	*a*	*b*	*c*
Baseline	~	~	~	~	~	~
Option 1	+	>	+	+	+	+
Option 2	++	>>	++	++	+	+
Option 3*:* Sub-option 3.A	+++	>>>	+++	+++	+	+
Option 3*:* Sub-option 3.B	+++	>>>>	++++	+++	+	+

266 Scores on effectiveness build on the extent to which the impacts screened in section 6 contribute to the achievement of the specific objectives. Scores on costs cumulate here both costs on service providers and on public authorities.

Impacts assessed	***Baseline***	***Option 1***	***Option 2***	***Option 3***
Economic impacts				
Functioning of the Internal Market and	~	+	++	+++

[136] Screening against Tool 27 in the Better Regulation toolbox, and the Commission's policy on Internet Governance (COM (2014) 072 final)

competition				
Costs and administrative burdens on digital services	~	>	>>	>>[137] / >>>[138]
Competitiveness, innovation, and investment	~	+	++	+++
Costs for public authorities	~	>	>>	>>>
Trade, third countries and international relations	~	+	+	+
Social impacts				
Online safety	~	+	++	+++
Enforcement and supervision by authorities	~	+	++	+++
Fundamental and rights (as laid down in the EU Charter)				
Freedom of expression (Art 11)	~	+	++	+++
Non-discrimination, equality, dignity (Art 21, 23,1)	~	+	++	+++
Private life and privacy of communications (Art 7)	~	+	+	++
Personal data protection (Article 8)	~	~	~	~
Rights of the child (Art 24)	~	+	++	+++
Right to property (Art 17)	~	+	+	+
Freedom to conduct a business (Art 16)	~	+	+	+
User redress	~	+	++	++
Overall	~	+	++	+++

7.2.1. Effectiveness

7.2.1.1.First specific objective: ensure the best conditions for innovative cross-border digital services to develop

267 The comparison of options against the first specific objectives rests primarily on the economic impacts of the options on service providers.

268 The first option improves the conditions for innovative online platforms to emerge in the Union by harmonising across the single market the due diligence obligations imposed on platform services for tackling illegal activities of their users. It also has positive impacts on hosting service providers and online intermediaries. The first option requires costs for service providers, in particular online platforms, but these remain proportionate to the capacities of the companies. The most significant costs are variable costs from the running on the notice and action system, and, consequently, they are proportionate to the risks services providers bring.

269 It answers to the most acute and current concerns Member States are raising at this point in time and improves innovation opportunities in the short term. It would also establish a level playing field between European companies and services offered from outside the Union, otherwise not subject to the same rules and costs when targeting European consumers. The positive impacts of the option with regard to addressing the legal

[137] For all digital services, costs are equivalent with those in Option 2

[138] While Option 3 requires further obligations triggering higher costs than option 2, these are circumscribed to a narrow population of very large platforms; they are proportionate to the financial capacity of the very large companies generally captured by the scope of the definition.

fragmentation in the single market might not endure in the medium- to longer-time horizon, since it harmonises the core, yet limited set of measures and relies on case law and self-regulatory measures for addressing emerging concerns.

270 The second option would significantly improve the effectiveness of the intervention by providing more legal certainty to all online intermediaries and removing disincentives for service providers to protect their services from illegal activities. This can bring relief in particular to innovative start-ups and small service provider. Compared to the first option, the second option will further improve the mechanic in the cooperation and trust between Member States authorities through a reinforced and more agile cooperation mechanism.

271 The third option would similarly significantly improve the conditions for the provision of services in the single market. It would establish a European governance system for the supervision and enforcement of rules fit for solving emerging issues and, importantly, able to appropriately detect and anticipate them. This should maintain a long-lasting trust and cooperation environment between Member States and offer technical assistance to ensure the best supervision of services across the Union. It would also calibrate these efforts and target them towards those services producing the biggest impacts. Overall costs for the majority of companies would remain comparable to those in option 2. This would also ensure proportionality of measures, to create the necessary space for start-ups and innovative companies to develop.

7.2.1.2.Second specific objective: maintain a safe online environment, with responsible and accountable behaviour from online intermediaries

272 The first option would bring a significant improvement to the baseline, in establishing the core measures for tackling illegal activities online and ensuring a consistent level of protection across all services and covering all types of illegal behaviours.

273 The second option would be expected to produce strong effects in this regard by stimulating targeted and appropriate measures from service providers. Importantly, it would offer an even stronger and responsive cooperation across Member States, supporting the protection of all European citizens both when online intermediaries or other digital services are concerned. It would also extent the scope of concerns tackled by empowering users to better interact with the platforms' environment, e.g. with regard to ads they see on online platforms.

274 For the third option, in addition to the features of option 2, would include stronger obligations and significantly more robust oversight on very large online platforms. This targets a stronger intervention towards service providers where the highest societal risks emerge, while ensuring that smaller online platforms can effectively address illegal content emerging on their services and can also be part on a voluntary basis of codes of conduct. The flexible co-regulatory environment to address in an adapted and speedy manner all emerging issues, would ensure that urgent, palpable results can be achieved, including in crisis situations. This would also be coupled with an effective and well calibrated European governance for enforcement and supervision. The overall effectiveness of sub-option 3.A and 3.B are comparable in this regard, while it is expected that, in the longer-term, option 3.B could deliver a more robust framework for intervention, whereas option 3.A providers for an immediately functional and effective enforcement structure.

7.2.1.3.Third specific objective: empower users and protect fundamental rights online, and freedom of expression in particular

275 The first option would significantly improve the current situation by affording users with the necessary due process rights and provisions for defending their rights and interests online.

276 The second option would in addition give users more agency and information online (e.g. with regard to recommended content or ads online) and an overall better environment for seeking information, for making choices, for holding opinions and participating in democratic processes.

277 The third option would importantly create a risk management framework that includes considerations for fundamental rights, including freedom of expression, where very large platforms are concerned. This ensures that, in particular in those 'public spaces' for exchanges, more robust safeguards are in place. This approach is also accompanied by adapted supervisory powers and capabilities for authorities in the context of a solid European governance. This would ensure both that issues are detected, and a co-regulatory framework for solving them as they emerge.

7.2.1.4.Fourth specific objective: establish the appropriate supervision of digital services and cooperation between authorities

278 The first option would enhance the baseline by establishing a common regulatory benchmark against which Member States can supervise online platforms and further streamlining the cooperation process for supervising the due diligence obligations on online intermediaries.

279 The second option would further enhance the supervision of all digital services and would offer a robust platform for cooperation across Member States as well as within each Member State.

280 The third option would offer an effective mechanism for supervision and cooperation, fit to anticipate future problems and address them effectively. This would rest on a European governance, ensuring that information and capability asymmetries between authorities and platforms are not impeding on effective supervision. It would afford the appropriate oversight powers to authorities and facility access to information to researchers ensuring that issues can be detected as they emerge. Under sub-option 3.A, an agile supervisory system would be set up immediately within the Commission, coupled with a tight structure for the exchanges between Member States' new digital services coordinators. Under sub-option 3.B, the supervisory structure with an EU body would give statutory powers to the EU Board.

7.2.2. Efficiency

281 The costs for each of the three options are proportionate to their effectiveness in achieving the four specific objectives.

282 The first option comes with lower costs on service providers and an expectation for higher costs on authorities to ensure a better supervision than the current situation, while creating significant efficiency gains in the cross-border cooperation.

283 The second option entails similar costs for service providers and is expected to lead to comparable costs on authorities, including efficiency gains through the cooperation

system. At the same time, the option is globally more effective than the first option at comparable costs.

284 The third option is similarly costly for all digital services, but requires higher compliance costs from a relatively small number of very large platforms. In what concerns authorities, it includes significant efficiency gains thanks to the cooperation mechanism, as well as higher costs for the effective supervision of services, including at EU level. In sub-option 3.A, a series of costs are streamlined by absorbing into the Commission's structure most of the investigative, advisory and enforcement EU-level powers. Under sub-option 3.B, the overall costs are higher, since the new agency needs to ensure its own administrative operations and does not directly benefit from the wider pool of expertise of the Commission. .

7.2.3. Coherence

7.2.3.1.With the Digital Markets Act

285 This initiative is coupled with an intervention to ensure a competitive digital economy and in particular fair and contestable markets. The Digital Markets Act intervention focuses on large online platforms, which have become gatekeepers and whose unfair conduct in the market may undermine the competitive environment and the contestability of the markets, especially for innovative start-ups and scale-ups.

286 Both initiatives contribute to shared objectives of reinforcing the single market for digital services, improving the innovation opportunities and empowering users, and improving the supervision over digital services. They complement each other in covering issues which are different in nature. The two initiatives should also reinforce each other in what concerns those very large online platforms falling in scope of both sets of measures, in particular in what concerns empowering users, but also in correcting business incentives for acting responsibly in the single market.

287 The definition of very large platforms falling in scope of the asymmetric obligations in option 3 is different in nature and scope from the 'gatekeeper' platforms considered for the Digital Markets Act. For the latter, the criteria will relate to the platforms' economic power in the market place while in the case of the option 3 analysed here, large platforms are understood as those which serve as *de facto* public spaces in terms of numbers of users. Consequently, not all very large platforms are expected to also be gatekeeper platforms, but many will likely fall also in that category under the Digital Markets Act.

288 All three options are fully coherent with the second initiative. The second and, to a larger extent, the third one, are further complementary with the second intervention, in particular by enhancing transparency and user agency with regard to core features of online platforms such as recommender systems and online ads.

7.2.3.2.Other, sector-specific instruments

289 The objectives of the instrument are fully aligned with the sector-specific interventions adopted and/or proposed by the Commission, such as the AVMSD, the Copyright Directive, and the proposed Regulation on terrorist content. Each of the three options would complement these initiatives, but would not seek to modify them.

290 For example, measures on all the proposed options would complement the obligation of a notification system set for video-sharing platforms in the AVMSD with more detailed requirement, with regard to transparency obligations and user complaints, and extending

their application horizontally to all types of online platforms and for all types of illegal content.

291 The Copyright Directive would remain a *lex specialis* with regard to the liability exemptions for certain types of platforms. At the same time, certain new obligations in the options, such as a harmonised notice and action procedure as well as various transparency obligations, will further enhance enforcement of the copyright acquis and help the fight against online piracy.

292 The three options are also fully compatible and coherent with the Platform to Business Regulation. In particular where the redress and complaint mechanisms for business users restricted by the platform is aligned with the provisions in the three options, and the Regulation allows for exceptions from the conditions its sets for restrictions on the business user of an online intermediation service in connection to illegal activities (see recital 23).

293 All the options would also provide for an effective cooperation and supervision system, with different degrees of impacts (see 6.1.1 and 6.2.2) which could further support sector-specific cooperation.

7.2.3.3. Coherence with Internet principles and the technical infrastructure of the internet

294 All three options are fully aligned and reinforce the principles of the open internet and the technical infrastructure of the network. This supports both the competitiveness of these sectors, but also, importantly, their resilience and their role in maintaining an open internet and protect their users' rights.

7.2.4. Proportionality

295 The three options follow the same principle of proportionality and necessity of an intervention at EU level: a fragmented approach across Member States is unable to ensure an appropriate level of protection to citizens across the Union, and the supervision of services would remain inconsistent. However, the effectiveness and proportionality of the third option in reaching the objectives is superior, not least in light of a future-proof intervention, allowing the supervisory system to respond to emerging challenges linked to the supervision of digital services and preventing future re-fragmentation of rules. Where the third option imposes sanctions, these are proportionate to the harms posed by the very large platforms concerned.

8. PREFERRED OPTION

296 Against this assessment, the preferred option recommended for political endorsement is the third option. This option would best meet the objectives of the intervention and would establish the proportionate framework fit for adapting to emerging challenges in the dynamic digital world. It would set an ambitious governance for digital services in Europe and would reinforce the single market, fostering new opportunities for innovative services.

297 It would also appropriately manage systemic risks which emerge on very large platforms, while establishing a level playing field for smaller players – both in terms of setting a core set of obligations to make sure online safety and fundamental rights are consistently protected online, and in making sure that all services targeting the European single market comply with the same standards of protection and empowerment of citizens.

298 The preferred option, while preserving the geographical scope of the E-Commerce Directive for its core provisions, would in addition set a gradual and proportionate set of due diligence obligations for different digital services, also applicable to services established outside the Union but offering services in the single market, as follows:

INTERMEDIARIES	HOSTING SERVICES	ONLINE PLATFORMS	VERY LARGE PLATFORMS
Transparency reporting			
Requirements on terms of service and due account of fundamental rights			
Cooperation with national authorities following orders			
Points of contact and, where necessary, legal representative			
	Notice and action and information obligations		
		Complaint and redress mechanism and out of court dispute settlement	
		Trusted flaggers	
		Measures against abusive notices and counter-notices	
		Vetting credentials of third party suppliers ("KYBC")	
		User-facing transparency of online advertising	
			Risk management obligations
			External risk auditing and public accountability
			Transparency of recommender systems and user choice for access to information
			Data sharing with authorities and researchers
			Codes of conduct
			Crisis response cooperation

299 Sub-option 3.A is recommended as the preferred option for the EU-level governance by virtue of its speedy feasibility and urgent application, with a comparable effectiveness to 3.B in the short to medium term.

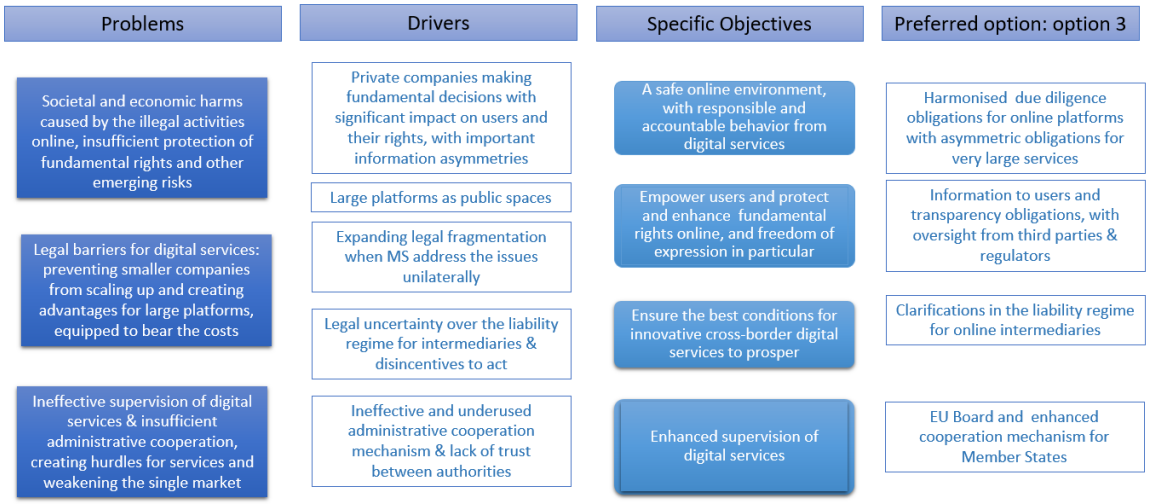


Figure 6 Intervention logic for the preferred option

9. REFIT (SIMPLIFICATION AND IMPROVED EFFICIENCY)

Table 7 REFIT cost savings for the preferred option

REFIT Cost Savings – Preferred Option(s)		
Description	***Amount***	***Comments***
Coordination and cross-border cooperation costs for national authorities will be significantly streamlined through the Clearinghouse system and the EU body	Quantitative estimates cannot be clearly established, as current costs vary from one MS to another, and gains and expenditure under the preferred option will depend on the MS' supervisory role for digital services and volume of requests to be processed	Concerns mostly national authorities in Member States
Core elements of the harmonising measures: due diligence obligations for online intermediaries	Between EUR 400.000 and EUR 15 mil for a medium-sized company, per year	Concerns hosting service providers, in particular online platform companies established in the Union

10. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

300 The establishment of a robust system for data collection and monitoring is in itself one of the core impacts pursued by the preferred option. This includes both the enhanced ability to monitor and account for the functioning of the cooperation across Member States' authorities, and the supervision of digital services.

301 Several monitoring actions should be carried out by the Commission, in evaluating continuously the effectiveness and efficiency of the measures.

Table 8 Summary of monitoring actions and indicators

Specific objectives	***Operational objectives***	***Key performance Indicators***	***Monitoring and indicators***
1. Best conditions for innovative, cross-border digital services to develop	Harmonised application of due diligence obligations for online platforms	Numbers and diversity of infringements and services concerned	Monitored through the reported data from the Clearing house system, with qualitative indications based on requests for assistance from Member States, response rates and resolutions.
		Number of derogation requests from MS (target: none – to be monitored)	
	Legal certainty and consistency in enforcement with regard to the due diligence obligations and the legal clarity in the liability regime for online intermediaries	Number of laws adopted derogating (target: none)	Reports from Member States through the cooperation under the EU Board
		EU start-ups and SMEs emerging in the single market;	Monitoring of the evolution of CJEU case law, national case law and complaints resolved in out of court dispute resolution mandated by the act.
		Economic indicators for cross-border trade (measured against projected increase of 1% to 1.8%)	
	Mitigate and prevent further burdensome legal fragmentation for digital services		Monitoring co-regulatory frameworks launched under the, their reported outcomes and the extent to which they address the underlying concerns and cover all relevant digital services and social

			partners.
2. Safe online environment, with responsible and accountable behaviour from digital services	Effective application of the due diligence obligations by service providers Effective actions by law enforcement	Strong stakeholder views, in particular from civil society, that stringent content removal KPIs incentivise over-removal of content. No unattainable 'zero tolerance' target Specific KPIs set for each co-regulatory framework Number of negative audits	Data reported by Member States supervising the systemic compliance of service providers – as collected through the Clearinghouse Number, complexity and effectiveness of cases pursued at EU level
3. Empower users and protect fundamental rights online	Compliance from service providers with due diligence and transparency obligations Investigations, audits and data requests from authorities, researchers and independent auditors	Number of complaints for content removal escalated to out of court disputes and authorities and leading to reinstatements Number of negative audits	Data reported by Member States through the Clearing house Monitoring of transparency reports, ad archives and compliance with specific requests from authorities and independent audits of service providers
4. Appropriate supervision of digital services and cooperation between authorities	Effective supervision and enforcement by Member State of establishment Responsive and effective cross-border cooperation	Response time from Digital Services Coordinators to requests from other Member States (target: no more than 10% over the 1 month deadline)	Monitored through the reported data from the Clearing house system, with qualitative indications based on requests for assistance from Member States, response rates and resolutions. Reports from Member States through the cooperation of the EU Board

302 The legal act would set the overall legal framework for digital services. It should be designed to remain valid in the longer term, allowing for sufficient flexibility to address emerging issues. Consequently, it does not necessitate a short-term review clause in itself.

303 Instead, the effectiveness of the instrument is likely to be strictly dependent on the forcefulness of its enforcement. For digital services to behave responsibly and for the framework of the single market to be a nourishing environment for innovative services, establishing and maintaining a high level of trust is paramount. This concerns as much the Member State level supervision of digital services, as the cross-border cooperation between authorities, and, where necessary, infringement procedures launched by the Commission. Yearly activity reports of the EU Board should also be compiled and made publicly available, with sufficient information on its operation and the cooperation and outcome indicators as presented in the table here-above. An evaluation of the instrument should be conducted within five years from the entry into force.