Digital Services Act Package

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Digital Services Act: furthering the single market and clarifying responsibilities for digital services

Accompanying the document

[...]

[...]
Table of contents

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT ............................................................... 1

2. PROBLEM DEFINITION ................................................................................................................... 2
   2.1. Context and scope ..................................................................................................................... 2
   2.2. What are the problems? ............................................................................................................. 4
   2.3. What are the problem drivers? ................................................................................................ 15
   2.4. How will the problem evolve? ................................................................................................ 21
   2.5. Problem tree ............................................................................................................................ 22

3. WHY SHOULD THE EU ACT? ........................................................................................................ 22
   3.1. Legal basis ............................................................................................................................... 22
   3.2. Subsidiarity: Necessity of EU action ....................................................................................... 23
   3.3. Subsidiarity: Added value of EU action .................................................................................. 23

4. OBJECTIVES: WHAT IS TO BE ACHIEVED? ............................................................................... 23
   4.1. General objectives ................................................................................................................... 23
   4.2. Specific objectives ................................................................................................................... 24
   4.3. Intervention logic .................................................................................................................... 25

5. WHAT ARE THE AVAILABLE POLICY OPTIONS? .................................................................... 25
   5.1. What is the baseline from which options are assessed? .......................................................... 25
   5.2. Description of the policy options ............................................................................................ 26
   5.3. Options discarded at an early stage ......................................................................................... 31

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS? ........................................................... 32
   6.1. Economic impacts ................................................................................................................... 33
   6.2. Trade, third countries and international relations .................................................................... 37
   6.3. Social impacts ........................................................................................................................ 38
   6.4. Impacts on fundamental rights ............................................................................................... 39
   6.5. Environmental impacts ............................................................................................................ 44

7. HOW DO THE OPTIONS COMPARE? ............................................................................................ 44
   7.1. Criteria for comparison ........................................................................................................... 44
   7.2. Summary of the comparison .................................................................................................... 44

8. PREFERRED OPTION ...................................................................................................................... 48

9. REFIT (SIMPLIFICATION AND IMPROVED EFFICIENCY) ....................................................... 49

10. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED? ............................. 49

ENDNOTES ................................................................................................................................................. 51
<table>
<thead>
<tr>
<th>Term or acronym</th>
<th>Meaning or definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaborative economy platform</td>
<td>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.</td>
</tr>
<tr>
<td>Competent authorities</td>
<td>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;</td>
</tr>
<tr>
<td>Content provider</td>
<td>a user who has submitted information that is, or that has been, stored at his or her request by a hosting service provider;</td>
</tr>
<tr>
<td>CSAM</td>
<td>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</td>
</tr>
<tr>
<td>Digital service</td>
<td>used here as synonym to an information society service – see definition below</td>
</tr>
<tr>
<td>Erroneous removal</td>
<td>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.</td>
</tr>
<tr>
<td>Harmful behaviours/activities online</td>
<td>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 certain extent, subjective.</td>
</tr>
<tr>
<td>Hosting service provider</td>
<td>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</td>
</tr>
<tr>
<td>Illegal content</td>
<td>any information which is not in compliance with Union law or the law of a Member State concerned;</td>
</tr>
<tr>
<td>Illegal activity</td>
<td>any activity which is not in compliance with Union law or the law of a Member State concerned;</td>
</tr>
<tr>
<td>Illegal goods or services</td>
<td>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.</td>
</tr>
<tr>
<td>Illegal hate speech</td>
<td>The following serious manifestations of racism and xenophobia that must constitute an offence in all EU countries:</td>
</tr>
<tr>
<td></td>
<td>(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;</td>
</tr>
<tr>
<td></td>
<td>(b) public condoning, for a racist or xenophobic purpose, of crimes against humanity and human rights violations;</td>
</tr>
<tr>
<td></td>
<td>(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;</td>
</tr>
<tr>
<td></td>
<td>(d) public dissemination or distribution of tracts, pictures or other material containing expressions of racism and xenophobia;</td>
</tr>
<tr>
<td></td>
<td>(e) participation in the activities of groups, organizations or associations, which involve discrimination, violence, or racial, ethnic or religious hatred.</td>
</tr>
<tr>
<td>Information Society Service</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Large online platforms</strong></td>
<td>online platforms reaching a certain level of users in the Union and having a significant societal and economic impact. Since the present consultation itself inquires about the distinctive features, the impact and the potential measures, which need to be taken in relation to such platforms, this definition should be understood more as a description of possible features that identify large online platforms.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Law enforcement authorities</strong></td>
<td>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;</td>
</tr>
<tr>
<td><strong>Notice</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Online platforms</strong></td>
<td>a variety of ‘hosting service providers’ such as search engines, 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.</td>
</tr>
<tr>
<td><strong>Online intermediary service</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Recommender systems</strong></td>
<td>refer to the algorithmic systems used by online platforms to give prominence to content or offers, facilitating their discovery by the users, typically based on the preferences of the user or similarity with content previously viewed. 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.</td>
</tr>
<tr>
<td><strong>Smart contracts</strong></td>
<td>software which executes the transfer of an asset upon fulfilment of pre-determined conditions (“if …then”). Smart contracts can transpose the terms of a written contract or they can exist stand-alone without a written contract.</td>
</tr>
<tr>
<td><strong>Trusted flagger/third party</strong></td>
<td>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;</td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>Refers, throughout the report, to any natural or legal person who is the recipient of a digital service</td>
</tr>
</tbody>
</table>
1. **INTRODUCTION: POLITICAL AND LEGAL CONTEXT**

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 is intended as a comprehensive package of measures for the provision of digital services in the European Union and seeks to address the challenges posed by online platforms, with two main initiatives:

- **First**, an intervention for deepening the single market for digital services and establishing clear responsibilities for online platforms to protect their users from the risks they pose, such as illegal activities online and risk to their fundamental rights;

- **Second**, an intervention consisting of combination of *ex ante* rules on prohibitions and obligations concerning clearly defined unfair practices by designated gatekeeper platforms and a competition-based market investigation regime to address emerging and existing market failures in digital markets.

This Impact Assessment covers the first set of measures and builds on the evaluation\(^3\) of the E-Commerce Directive\(^4\), annexed to the report.

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.

In the Communication ‘Shaping Europe’s Digital Future’\(^5\), 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.

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. The Council’s Conclusions\(^6\) 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 2\(^{nd}\) October 2020\(^7\).

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

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, including the United Kingdom, the United States, Australia, Canada, India, and many others.
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.

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 was 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’, ‘coaching services’, and “hosting services” – for third party content.

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, marketplaces or search engines, 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.

In response to the evolving digital landscape, several service-specific and sector-specific legal acts have complemented the ground rules by regulating different aspects of the emerging ecosystem e.g. online banking and payment services, telecommunication services, messaging services and, most recently, business-to-business relationships on online platforms and search engines, and the free flow of data rules. In addition, several issue-specific legal acts 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.

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.

More recently, the Commission has also taken a series of targeted measures, both legislative and self-regulatory, as well as coordinated enforcement actions in the framework of the Consumer Protection Cooperation Regulation (CPC), 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.

This impact assessment explores the changed nature, scale and influence of digital services. The assessment will track key drivers which have led to societal and economic challenges posed by the digital services ecosystem and outline the options to address them and improve the functioning of the digital single market.

2. Problem definition

2.1. Context and scope

Digital services 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:

- apps, online shops, e-games, online versions of traditional media (newspapers, music stores), Internet-of-Things

![Figure 1 Types of digital services](image-url)
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, search engines, 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.

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.

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. 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.

A study conducted for the European Parliament 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. Overall welfare gains from e-commerce are estimated to be between 0.3 and 1.7% of EU-27 GDP.

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 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, from user-generated content to video-on-demand.

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, with several types of intermediaries involved in the placement of ads.

The evolution is not limited to consumer-facing digital services, far from it. In particular, what concerns services 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 services such as DNS are a precondition for digital services to be effectively delivered to and accessed by internet users.

While online platforms present particular opportunities and concerns and are most prominently referred to, all these digital 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:

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.

Second, digital 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.

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.

Fourth, while 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.

Fifth, while there are approximately 11,000 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, search engines, 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.

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.

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 since the offset of the pandemics. At the same time, the 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.

Against this background, the Impact Assessment covers all types of digital services, the risks and harms they may represent, and the challenges they are facing in the Single Market. It also more narrowly analyses issues related to online intermediaries and online platforms in particular, since they present the biggest concerns and opportunities in the dissemination of information and sale of goods and services online.

2.2. What are the problems?

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

<table>
<thead>
<tr>
<th>Main problems</th>
<th>For whom is this a problem?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Main types of digital services concerned</td>
</tr>
<tr>
<td>1. Serious societal and economic risks and harms brought by digital services: illegal activities online, insufficient protection of the fundamental rights and other</td>
<td>Illegal activities and risks to fundamental rights: all types of digital services, with particular impacts where online platforms are concerned</td>
</tr>
</tbody>
</table>
2. Ineffective supervision of digital services & insufficient administrative cooperation, creating hurdles for services and weakening the single market

3. Legal barriers for digital services: preventing smaller companies from scaling up and creating advantages for large platforms, equipped to bear the costs

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 has been happening across 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.

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 particular if these are not used appropriately or not used at all.

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 mechanism of cooperation between Member States’ authorities is underspecified, which makes it unreliable for Member States. The evaluation shows that the existing mechanism, whose existence is still considered very relevant and important, requires further clarifications and reinforcements to ensure trust between Member States and an effective supervision and sanctioning of digital services in the country of establishment.

*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 regime for online intermediaries 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”, 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 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. In view of the significant developments of the digital economy and services, the question arises whether other types of intermediary services (e.g. virtual private networks, content delivery networks) can also benefit from the liability safe harbour. At the same time, some providers exercise a predominant influence over the hosted content, leading the user to confusion as to the identity or origin of the content he or she visits – 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\(^\text{21}\) 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 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.

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 today play 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**

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**

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 report on content removal figures. Even though such removals are usually based on standards of private community rules, possibly including not only illegal content but also harmful content and other content breaching the terms of service, the reported numbers will 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\(^\text{22}\), and 80% of products detected by customs authorities involved small parcels\(^\text{21}\), 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).\textsuperscript{24} For unsafe products, the Rapid Alert System for dangerous non-food products (Safety Gate/RAPEX) registers between 1850 and 2250 notifications from Member States per year.\textsuperscript{25} 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.\textsuperscript{26} 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,\textsuperscript{27} 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.\textsuperscript{28}

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.\textsuperscript{29} This trend is confirmed by the European centre network of hotlines, INHOPE, which indicate that images processed between 2017-2019 almost doubled.\textsuperscript{30} 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.\textsuperscript{31} As an example, Facebook reported 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 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 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.\textsuperscript{32}

To better contextualise the online component of such illegal activities, the Commission ran a Flash Eurobarometer survey 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)](image)

\textbf{Services concerned in the spread of illegal activities are diverse in nature and size}

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 misleading and scamming consumers, or by selling illegal products. This remains a persistent problem, and almost 80% of all notifications and assistance requests sent by Member States for cross-border issues concern infringements by such online services.
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. Further, such services are themselves built for optimising access to content or commercial offers, respectively, and can 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 biggest number of users can be reached and where the amplification of illegal content and activity is arguably most potent.

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.

Box 3: Types of digital services most used for illegal activities: examples

According to INHOPE, 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 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 volumes of content, 68% of Europol referrals were addressed to micro, small and unregistered companies in 2017.

b) Emerging systemic societal risks posed by online platforms

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’. 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).

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. Risks, however, go beyond the spread of illegal activities. Negative effects also stem from the amplification of content which is not per se, illegal, and the perpetuation of online behaviour which might be otherwise harmful: such as extreme selfies and instigation to violence or self-harm (harmful in particular to children and in the context of gender-based online violence), conspiracy theories, disinformation related to core health issues (such as the COVID-19 pandemics or vaccination), political disinformation, etc. The same amplification tools can also tilt consumer choice on marketplaces and have an impact on sellers’ ability to reach consumers. Certain practices may also have negative impacts on users’ freedom to make uncoerced political decisions and on authorities’ capacity to monitor and ensure political processes.

This amplification happens through the design choices in platforms’ ranking systems on embedded search functions (or on search engines), recommender systems, and through more or less complex advertising placement services, including micro-targeting.
Such issues stem from at least **two potential sources**: 

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

Micro-targeting with political advertising is also alleged to have similar effects, in particular in electoral periods, but evidence of actual impact in voter behaviour is not consistently conclusive. 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. Lack of transparency around political advertising is in itself a risk for fair electoral campaigns.

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.

It is clear that the dynamics of online interactions have an impact on real world behaviours. However, evidence on the extent of these impacts and the possible harms is incomplete and continuously evolving with several challenges which need to be addressed to ensure a better understanding of the phenomenon. Extensive academic research, 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.

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.

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. Some research projects and civil society experiments attempt to observe platforms’ algorithmic systems and their effects, 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.

c) **Fundamental rights are not appropriately protected**

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.

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 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 or documented evidence from war zones.

Some regulatory initiatives, such as the Platform to Business Regulation, obliges 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’), 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.

However, other users depend entirely 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 pandemics, 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).

It is virtually impossible to estimate in quantitative terms the scale of erroneous removals and blocks. 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.

In the Eurobarometer survey run by the Commission in 2018, 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.

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 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 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.

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.
At the same time, fundamental rights are also at risk when and users are prejudiced when service providers do not take any action, leaving content untouched that severely violates interests of others, including in cases where users have reported such content (see previous section a) here-above).

Who is affected and how?

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.

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.

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.

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 business practices and interests.

Stakeholders’ views

The majority of the stakeholders consulted indicate that, although the current legal framework has supported innovation from companies throughout the EU and allowed users to benefit from those services, some regulatory changes may be needed in light of the digital transformation of the last twenty years.

In the various consultations carried out in the context of this impact assessment, several stakeholders – such as civil society organisations, online platforms, national authorities and academia – underlined the increasing challenge raised by the volume of illegal online content and illegal goods sold online and acknowledged their negative impact on EU citizens.

More specifically, civil society organisations, industry associations and national authorities have carried out studies and coordinated test purchase investigations demonstrating an increasing amount of illegal goods available in the EU via online marketplaces. The studies also demonstrated that the vast majority of such illegal goods come from third countries. Moreover, public consultations show that the majority of citizens have come across illegal goods, services and content on online platforms several times, and users are not satisfied with the actions that platforms take to minimise risks.

At the same time, online intermediaries, civil society organisations, academia and national authorities emphasize that any new measure to tackle illegal content online should not unintentionally lead to unjustified limitations on citizens’ freedom of expression or fundamental rights to personal data and privacy. Civil society organizations and academia are particularly worried that automated tools might not guarantee the protection of fundamental rights due to illegitimate takedowns.
In this regard, consumer organisations consider that digital services have become an enabler for consumer law violations incentivised by a revenue stream from the sale, advertising or promotion of dangerous, unsafe, illegal products online. Such organisations strongly call for a special liability regime for online marketplaces, in case of failure to take adequate measures upon obtaining credible evidence of an illegal activity, failure to inform about the supplier of the goods or services, provision of misleading information or in case they have a predominant influence or control over their suppliers.

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

The supervision of digital services, including online platforms, is to a large extent uncoordinated and ineffective in the EU, despite the strategic importance of such services. The administrative cooperation framework set by the E-Commerce Directive for addressing cross-border issues is underspecified and inconsistently used by Member States. It was set at a time when the number, scale and impacts of the digital services was significantly lower than today. This fuels a lack of trust across Member States when it comes to supervising digital services 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 digital services.

Whereas digital services are instrumental 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:

First, a core failure in supervision of digital services stems from the lack of trust and cooperation among authorities in cross-border issues. Digital services are naturally borderless. 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. For a smooth functioning of the system, Member States need to trust that information society 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 Community citizens. However, the implementation failures of the underspecified cooperation mechanism designed in the E-Commerce Directive, have eroded trust between Member States.

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 process 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.

Absent an effective cooperation mechanism, 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.

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 intermediaries, the increasing challenges of supervising the underlying services they intermediate, such as accommodation or transport services, or websites conducting illegal activities online.

Third, authorities have very few levers for supervising services established outside of the Union, while such services are easily be 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**

Overall, all stakeholders recognise the fact that authorities play the central role in the fight against illegal activities online and in the effective application and enforcement of EU law. In this regard, national authorities, civil society organisations and brands associations emphasize the importance of coordination between all actors involved in the ecosystem.

Some civil society organizations highlight that robust and effective enforcement mechanisms for regulatory oversight are necessary, in particular to foster coordination between national authorities and to address issues with lack of transparency and inconsistencies within procedures.

Similarly, the majority of academics that have submitted their opinion in this regard call for strong enforcement to hold platforms to account and are in favor of a supervised regulator or authority to reconcile opposing needs and potentially sanction repeated failures. The regulatory oversight must be clear, foreseeable, proportionate, and fair.

Online intermediaries also consider that any regulatory oversight mechanism should be proportionate, increase legal certainty and follow a single market logic in ensuring the free provision of services.

National authorities emphasized the inadequacy of existing cross-border mechanisms and lack of oversight and cooperation between Member States. Cooperation between Member States is essential. The majority of respondents are in favour of assessing the feasibility of a unified European oversight agency, which could collaborate with national authorities, while others think that, in line with the subsidiarity principle, it might not be appropriate.

Generally, all categories of stakeholders consider that any new rule on digital services should ensure applicability and enforcement of measures to third country players providing their services to European users.

### 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 digital services at national level to supervise them and reduce harms. The resulting fragmented 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.

Some Member States are increasingly legislating to protect their citizens from those risks generated by digital services established in a different Member State. When digital services 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. This fragmentation is particularly concerning online platforms and the obligations imposed in some Member States with regard to their responsibilities, but other areas of fragmentation are also emerging, affecting other digital services (see driver 2.3.1).

The impact on digital service providers 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**

In a direct cost model, 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 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.

With the evolving fragmentation, these costs can have an impact on the over 11,000 potentially high-growth platforms established in the EU, out of which around 96% SMEs, more than half of which 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.

Across all sectors, the current state of the legal fragmentation is estimated 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 unique users for 31,084 web domains).

**Legal uncertainty**

Other important 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 behavior 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. Other services are also facing legal uncertainties, including concerns related to their very status as information society services, the obligations related to online advertising services, or the use of smart contracts (see Annexes 5, 6 and 12).

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. 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 cantisissuade businesses from expanding and growing in the single market.

**Stakeholders’ views**

Generally, all stakeholders agree that a horizontal harmonisation of rules for digital services in the European Union is necessary and that the trend towards Member States enacting varying legislation and rules around illegal content, goods and services has created undue burdens to companies, especially to SMEs.

Some business associations further explain that new digital services are often reluctant to set foot in different European markets due to diverging national legislations. Legal fragmentation, for example in the area of notice and action requirements, is considered as hindering the ability of start-ups to scale up and compete globally. In this regard, several stakeholders highlight the importance to address the current challenges at European level.

This issue is also recognised by national authorities, which agree with the need for a horizontal harmonised framework to tackle fragmentation stemming from national and EU legislation.

Moreover, numerous stakeholders highlight that the current framework for digital services requires some legal clarifications. For instance, according to some online intermediaries, the lack of clarity around the distinction between “active” and “passive” or the condition of “actual knowledge”, as provided for in the E-Commerce Directive, creates an incentive to refrain from engaging in reasonable proactive measures to tackle illegal activities. Therefore, platforms call for clear rules and responsibilities that do not disincentives their proactive actions to limit distribution of illegal content and goods online. Moreover, most stakeholders agree on the need to clarify the intermediary liability regime for new types of services, such as cloud services or CDN services.
2.3. **What are the problem drivers?**

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

76 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.

77 There 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.

78 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 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.

79 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*.’

80 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 (3 of the online intermediaries responding to the open public consultation), and are not equally reliable across services. 17% of respondents to an Eurobarometer survey, whose content was erroneously removed by online platforms, also said that they were never informed by the platforms about the reason for the removal.

81 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 to dissuade illicit sellers and to enable the enforcement of sanctions against them. On-boarding process 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.

The large online platforms release regular transparency reports. This practice has increased since the Commission’s Recommendation of 2018. 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 and removed. They are not standardised, use different definitions and different metrics for the data reported, and can hardly be compared across services.

Some online platforms are starting to set up additional structures in their decision-making on content moderation, with oversight boards 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.

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

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. With over half of the population in the EU using social media, reaching to nearly 90% for those aged 16-24, the effects of the design and standards on these platforms have an 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. Main marketplaces attract millions of sellers depending on them for reaching their audiences. 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.

The overwhelming majority of users are centralised today in a small number of online platforms. While precise data on the number of unique users is not available, available data shows the staggering differences of scale in the reach of the first few online platforms and the long-tail of other services. In the graph above, the average unique monthly users of a service are presented both for in-app and browser use (they are not necessarily cumulative, as same user could use both instances of the service) shows the staggering differences of reach across different types of platforms.

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. 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. 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.

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 flaws leading to unintended consequences with serious social impact, 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. 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\textsuperscript{83} and search engine optimisation\textsuperscript{84}

The societal risk of exposure to illegal content and activities is particularly high on large online platforms reaching a very wide audience. 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.

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. \textit{Legal fragmentation}

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)).

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.

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

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

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

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

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.

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.

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.

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 Avia Law, the recently notified Austrian draft law to combat hate speech online, the German draft law to protection of minors or the Italian “Airbnb” law.

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) or, increasingly, on responsibilities for online advertising intermediaries (see Annex 12).

2.3.4. **Regulatory gap: systemic issues are not appropriately addressed**

Systemic elements remain unaddressed by the regulatory framework. 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.

For certain types of illegal or suspicious activities, recent EU legal acts include set a series of targeted obligations on online intermediaries; They define specific legal obligations for issues such as copyrighted content, the sale of explosive precursor chemicals, and other types of illegal products subject to market surveillance. However, all these measures remain targeted to very specific concerns and they do not cover the systemic challenges brought by online platforms. The recently revised Audiovisual Media Services Directive, currently being transposed by Member States, includes a set of requirements for video sharing platforms but does not cover all online platforms.

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, the Product Safety Pledge, the Memorandum of Understanding on the sale of counterfeit goods on the internet, the Memorandum of Understanding on online advertising and intellectual property rights). 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.

Further, they will always remain targeted, whereas the scope of illegal activities and information, as defined in national and EU law, is much broader and broader, harmonised measures to tackle these concerns are missing. The only horizontal measures addressing all types of illegal content were covered by the Commission’s Communication from 2017 and, with more detail, the Recommendation of 2018 on measures to effectively tackle illegal content online, which encourages hosting service providers to implement accessible and user-friendly notice-and-action mechanisms.

These non-binding measures set out guidelines for all hosting services as regards illegal content, but the measures are 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 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.

With regard to online advertising services, 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. However, the provisions are limited to commercial communications and online advertising landscape has changed dramatically since the Directive was adopted. The responsibilities of ad intermediaries are not consistently clear and the disclosure obligations are outdated in relation to the type of information users need (see section 2.2.1).

The E-Commerce Directive does not prevent court or administrative authorities to issue injunctions against intermediaries to detect and prevent illegal activities, to the extent that they do not constitute a general monitoring obligation. However, it does not regulate the necessary conditions to be met. There is sector-specific legislation, such as in the field of intellectual property rights enforcement, but horizontal rules on the conditions and limits for such injunctions are missing. This has led to inconsistencies in the way national authorities and courts act against intermediaries, and results in further legal uncertainty for those.

2.3.5. Legal uncertainties and contradictory incentives

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

Uncertainties for digital service providers

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 within sector-specific rules or horizontal EU legal acts, such as the Services Directive. 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.

As regards the prohibition of prior authorisation requirements targeting information society services, the relationship between the E-Commerce Directive and more recent EU legislation, such as the European Electronic Communications Code (as regards number-independent interpersonal communication services) or AVMSD (for video-sharing platforms) may still pose some interpretative difficulties.

Other areas of legal uncertainty are emerging from somewhat outdated formulations in the E-Commerce Directive in the way they cover today e.g. advertising services, or new types of electronic contracts (smart contracts based on distributed technologies), etc. As the underpinning technologies develop, this could evolve into major blockages for the development of such digital services in the single market.

Liability regime for online intermediaries

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.
First, since the adoption of the E-Commerce Directive, services have evolved considerably, in all layers of the internet stack. The evaluation report of the Directive (see Annex 5) concluded on a lack of clarity, which is only partly remedied by the evolving case law of the Court of Justice\textsuperscript{103}, as regards the application of the liability exemption to infrastructure services. This includes, for instance, content delivery networks, registrars and registries in the DNS system, or, higher in the stack, search engines.

Second, 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\textsuperscript{104} – 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 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 Øe in a case which is currently pending before the Court\textsuperscript{105}. 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.

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.

Fourth, the E-Commerce Directive does not contain explicit rules regulating the liability of a service provider which takes down content in good faith as a result of a notice, or proactively, because it considers that it is illegal - and the content later turns out to be not illegal. Last, the Directive does not define the notion of ‘actual knowledge’ – nor under which conditions a notice can trigger such actual knowledge.

2.3.6. Limited cooperation among Member States and lack of trust

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.\textsuperscript{106}

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 States)\textsuperscript{107}.

In several surveys over the last years\textsuperscript{108}, 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, 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.

A much larger number of requests have escalated to restrictions through laws covering information society services. Between 2004 and 2020, 659 such laws were notified to the Commission under the TRIS procedure. The Commission analysed the notifications and issued comments on 131 occasions, and detailed opinions on 39.

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.

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.

2.4. How will the problem evolve?

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.

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.

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.

Member States will continue to legislate unilaterally and increasingly so with extraterritorial provisions, in addressing the emerging challenges of digital services, stemming from the use of ever-evolving technologies, like artificial intelligence or blockchain, or from the risks posed by new business models. 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.

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.

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]

3. Why should the EU act?

3.1. Legal basis

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.

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).

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 digital 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 digital services and cooperation between authorities at EU level, therefore supporting trust, innovation and growth in the Digital Single Market.
The new legal instrument would build on the principles of the E-Commerce Directive. Therefore, depending on the choice of policy option, as detailed below, and of legal technique, the three legal bases presented above should be considered, either together or focusing on an intervention based solely on Article 114 of the Treaty.

3.2. **Subsidiarity: Necessity of EU action**

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.

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**

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.

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.

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.

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**

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

This objective is specifically linked to the first set of problems identified: the aim is to ensure that the online environment is a safe place for all citizens, for legitimate expression and for businesses to develop in observance of the rights and values of a democratic society. In close connection to achieving the following specific objective, this objective 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 abused for conducting illegal activities and in cooperating with authorities, and that they do not lead themselves to societal harms.

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

In line with the general objective, a first specific objective is to establish the best conditions for the emergence and the scaling-up of digital services in Europe, as a strategic sector, enabling the digital economy and beyond. This objective is specifically linked to a predictable legal environment across the entire single market, where the cross-border provision of services is as frictionless as possible and does not generate a significant duplication of costs. It is also linked to legal clarity and proportionality of obligations and requests from digital services, accounting for the differences in capability, resources but also impacts and risks raised by small, emerging services compared to very large, established ones.

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

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. This involves responsibilities for authorities as much as for private companies, in particular online platforms becoming ‘public spaces’ for information sharing, for communication or conducting businesses. Promoting freedom of expression online is a key objective, both in terms of 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. User agency in forming opinion and understanding their informational environment is also paramount for their democratic participation, freedom to hold opinions and freedom of assembly. Other fundamental rights and values must also be ensured by the future regulatory framework: 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 digital services and cooperation between authorities*

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

<table>
<thead>
<tr>
<th>Problems</th>
<th>Drivers</th>
<th>Specific Objectives</th>
<th>General Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Societal and economic harms caused by the illegal activities online, insufficient protection of fundamental rights and other emerging risks</td>
<td>Private companies making fundamental decisions with significant impact on users and their rights, with important information asymmetries</td>
<td>A safe online environment, with responsible and accountable behavior from digital services</td>
<td>Ensure the functioning of the single market for digital services</td>
</tr>
<tr>
<td>Legal barriers for digital services: preventing smaller companies from scaling up and creating advantages for large platforms, equipped to bear the costs</td>
<td>Large platforms as public spaces</td>
<td>Ensure the best conditions for innovative cross-border digital services to prosper</td>
<td></td>
</tr>
<tr>
<td>Ineffective expression of digital services &amp; insufficient administrative cooperation, creating hurdles for services and weakening the single market</td>
<td>Expanding legal fragmentation when MS address the issues unilaterally</td>
<td>Empower users and protect and enhance fundamental rights online, and freedom of expression in particular</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal uncertainty over the liability regime for intermediaries &amp; disincentives to act</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ineffective and underused administrative cooperation mechanism &amp; lack of trust between authorities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enhanced supervision of digital services</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5 Intervention logic

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

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

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 the Directive on Copyright in the Digital Single Market, as well as the recently amended Audiovisual Media Services Directive and the Terrorist Content Regulation, once adopted.

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.

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. A patchwork of national measures would not effectively protect citizens, given the cross-border and international dimension of the issues. The proliferation of illegal goods sold online and the dissemination of illegal content would likely continue, and no harmonised safeguards against over-removal of legal content would exist. At the same time, there would be no safeguards established for protecting users’ rights. 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.
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

A wider set of options were considered at the scoping phase of the impact assessment, in particular in relation to: the obligations of online platforms, the liability regime of online intermediaries, the supervision of digital services 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.

In addition to the baseline, three packages of options are retained for assessment, which include both legislative and self- and co-regulatory measures.

The three retained options are the following:

1. Limited measures against illegal activities, laying down the procedural obligations for 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.

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 EU governance with reinforced oversight and enforcement.

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
<th>Option 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Limited measures against illegal activities</strong></td>
<td><strong>Full harmonisation</strong></td>
<td><strong>Asymmetric measures and EU governance</strong></td>
</tr>
</tbody>
</table>

**Obligations on online platforms**

- **Due diligence obligations** for a fit and proper operation: 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 recommender systems and advertising

- **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 recommender systems and 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, accountability of executive boards, participation in co-regulatory efforts to mitigate emerging risks
1. **Option 1 – Limited measures against illegal activities**

The first policy option establishes a set of **due diligence obligations** concerning tackling illegal activities online on all online platforms, 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 the online platforms in accordance with harmonised standards. This is coupled with an obligation to inform notifiers on the follow up given to the notification and information to users if their content is removed as well as specific actions around repeat offenders. The information obligation are coupled with an obligation to put in place an **accessible and effective complaint and redress mechanism** internal to the company (counter-notice) and the availability of out of court dispute mechanisms.

- **Know Your Business Customer** (‘KYBC’) – Online marketplaces 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. This may include information to users about EU legal requirements, i.e. on products.

- **Cooperation obligations** – Obligations to cooperate with public authorities and trusted third parties. This obligation includes fast-track procedures for notices from authorities (sent in accordance with legal standards).

- **Fundamental rights by design** – This includes the obligation to adopt a ‘fundamental rights by design’ approach when implementing the due diligence obligations.
Concerning the supervision of digital services, this option would enhance the cooperation mechanisms established in the E-Commerce Directive by setting up an enhanced ‘Digital Clearing House’. This agile system would 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.

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 under certain conditions, such as reaching a certain threshold of a minimum number of monthly European users. Such services would not be in scope of other rights or provisions of the new act and/or the E-Commerce Directive.

Stakeholders’ views
Generally, all consulted stakeholders call for a horizontal harmonisation of the framework for digital services in the EU, whilst persevering the fundamental principles of the E-Commerce Directive.

Online intermediaries advocate for a harmonisation of notice and action procedures across the EU. Most businesses also call for the establishment of minimum information requirements for a notice to be actionable. Some businesses believe that persistent abusers of the notice and action procedures should be held accountable and that intermediaries should be permitted to ignore their notices on the grounds that such notices do not convey “actual knowledge”.

Associations of businesses and trade organisations are also largely in favour of clear and harmonised notice and action obligations. Furthermore, most contributions of media and audiovisual associations argue for the need of clear policy against ‘repeated infringer’, and also for the regulation of the notion of ‘trusted flaggers’.

The majority of the civil society organisations emphasize that harmonised notice and action procedures are necessary. Most of them also indicate that minimum requirements for notices should be specified in law and that human moderators are an important component. This was also stated by contributions from academia.

Online intermediaries largely recognise the role of transparency, especially as an essential component of platforms’ accountability and trust to their users. This category of stakeholders also agree that different types of content and audience may merit different levels of transparency. Some online intermediaries consider that a transparency obligation can be best achieved by establishing a requirement for regular reporting. However, this category also highlight the possible risks of too far reaching transparency obligations, such as infringing upon trade secrets or intellectual property rights.

There is a broad support for increased transparency from associations of businesses and trade organizations. The majority of retail associations highlight the need for platforms to inform consumers who have previously bought an illegal or dangerous product that they have been exposed to illegal goods, following an appreciation by authorities. Concerning online marketplaces, some stakeholders flagged the need to verify the sellers (‘Know-Your-Business-Customer’) in order to inform consumers who purchased a fake product and to increase the efficiency of enforcement.

The majority of the civil society organizations identifies the lack of transparency as one of the major problems. For them, information asymmetries between platforms and users should be diminished. This position is also supported by academia.

Even platforms acknowledge possibility for more transparency, but warn against possible implications in terms of compromising commercially-sensitive information, violations of privacy or data disclosure laws, and abuse from actors that could game their systems.

Contributions from media/audiovisual associations agree that the E-Commerce Directive should not be reopened but rather complemented and that any regulatory intervention on this needs to preserve and build on the existing sectorial regulation.

2. Full harmonisation

This option would include the same due diligence obligations for all online platforms as those foreseen in option 1.

In addition, this option would impose on online platforms further transparency obligations towards their users, specifically regarding:
- Amplification systems which suggest the information users see online, such as content recommender systems – Obligations of transparency enabling users to understand why, and influence how information is being presented to them.

- Advertising systems – modernised transparency obligations extending the scope of the requirements in the E-Commerce Directive to all types of advertising (all ads placed online through online ad intermediaries, not just commercial communications, but also e.g. issue-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 (type of advertising –e.g. targeted, contextual - and, if applicable, targeting information).

156 This option would also allow national authorities to issue well specified requests for information necessary for the supervision of the underlying service intermediated by platforms (e.g. registration numbers of accommodation services, or labour law data of transport services).

157 Concerning the liability of intermediaries, option 2 would adapt the existing legal framework to incentivise hosting services, including online platforms, to take additional, proactive measures to address illegal activities: the intervention would clarify that such proactive measures do not, in themselves, remove intermediaries from the scope of the liability exemptions under the E-Commerce Directive. In addition, the option would harmonise certain conditions for court and administrative orders to impose measures for the removal and detection of illegal content, goods or services by intermediaries.

158 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, as well as with ensuring the cooperation interface for smoother cross-border assistance through the Digital Clearing House.

**Stakeholder views**

Online intermediaries call for introducing a clearer framework in relation to voluntary measures that are taken in good faith and should not lead to losing the liability safe harbor.

The majority of the civil society organizations highlight the importance of transparency with regards to algorithmic systems of recommendation and automated content moderation.

Regarding online advertising, more transparency is considered by many stakeholders necessary on the identity of the advertiser, on how it is personalised (e.g. ‘why am I seeing this ad’ features), and on the actions taken to minimise the diffusion of illegal content/goods/services. Political advertising and microtargeting is considered to raise specific and urgent challenges.

Online intermediaries generally consider that any new measure should avoid being overly prescriptive as to the use of specific tools or technologies in the context of content moderation. Not all platforms might be equal in their capacity to implement and run such technologies.

Some telecommunication operators and associations of businesses indicated the lack of transparency in automated systems. This is also highlighted by civil society organizations which emphasize the importance of transparency with regards to algorithmic and recommender systems (for automated content moderation), as transparency is necessary for building accountable algorithms.

Online intermediaries consider that any regulatory oversight mechanism should be proportionate, increase legal certainty and be based on the internal market principle and that the question of dedicated authority for the digital market should be carefully assessed. Online intermediaries also emphasize the importance of coordination between national authorities and between all actors involved in the ecosystem.

Many stakeholders call for improved cooperation between authorities in different Member States and highlight the importance of sharing data with law enforcement authorities, in particular for rogue traders.

Moreover, the vast majority of the stakeholders consulted advocate for an extension of the scope of application of any future legislation on digital services to players established outside the EU and which are offering their services to the EU.
3. Asymmetric measures and EU governance

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.

The additional set of enhanced obligations on very large online platforms reaching a significant number of Europeans are proportionate to the systemic impacts and risks these large platforms represent for society and the business environment, as well as to their capacities. Such obligations include:

- enhanced transparency and reporting obligations with regard to content moderation, content amplification and online advertising activities at the request of competent supervisory authorities;
- obligations to ensure access to data for researchers and regulators, including maintenance and broad access to ad archives;
- independent systems audit;
- voluntary participation in adaptive and responsive codes of conduct to mitigate emerging risks, but coupled with and obligation to ensure reporting on outcomes, or participation in crisis management protocols.

A very large platform prone to the additional obligations should have a significant reach among Europeans. An initial threshold is set at 10% of the EU population, as an indication of reach, when the platform is present in more than one Member State. Given the changing evolution of risks brought by platforms, the Board (see below, paragraph 164) could issue opinions for adapting the threshold, enacted through delegated acts. Digital coordinators can request reports from platforms on the number of unique users estimated to be reached.

Concerning the liability of intermediaries, option 3 includes several additional measures to adapt the 20-year-old legal framework to the realities of today’s digital services. Apart from incentivising voluntary actions to detect and act against illegal activities, as per Option 2, this option further clarifies the liability regime for online intermediaries to ensure legal certainty and foster innovation. It clarifies that, where a service has predominant influence over the content/information, that service cannot benefit from the liability exemption. It further clarifies the status of new types of services as intermediaries (e.g. content distribution networks, registrars and registries), many of which have been difficult to fit under the original categories and definitions of the E-Commerce Directive.

Similar to option 2, it harmonises certain conditions for court and administrative orders to impose measures for the removal and detection of illegal content, goods or services by intermediaries.

For the supervision of digital services, apart from the Digital Clearing House and the national Digital Coordinators, Option 3 also establishes a robust and modern governance structure at EU level. The structure includes a new EU Board established through the legal act as an independent body of the Union. It includes structural participation from national Digital Coordinators and delegates of the Commission, and a Secretariat to support its work. The Board and its Secretariat offer Member States’ authorities technical and coordination assistance for inspections and oversight, facilitate and oversee the administrative cooperation through the Digital Clearing House, and issue guidance on evolving challenges. The new governance structure for digital services also includes EU level competences by allowing the Commission, upon initiative of the Board or in case of substantiated evidence, to issue instructions for the coordination of the Digital Coordinators and, in specific circumstances, also directly enforce the due diligence obligations on providers. National authorities and the Board can request infringing services to take corrective measures and, absent corrective action, apply severe sanctions for systematic non-compliance, including other sanctions beyond mere financial fines, where these risk not being deterrent.
Stakeholders’ views

Online intermediaries are very supportive of maintaining the current liability exemption as defined in the E-Commerce Directive since it is considered as essential for the development of an innovative digital economy and the freedom of expression. Some businesses ask for the clarification of conditions such as ‘actual knowledge’.

Some business organisations and startups consider that some of the provisions proposed in possible new legislation should only apply only to ‘dominant’ intermediaries. According to them, limiting some obligations to large players would help targeting legal obligations to where problems actually occur and supports the successful development of competing alternative services and business models, as well as ensuring a fair and proportionate responsibility not-for-profit and community-led platforms that are more respectful of users’ rights. Some telecommunication operators also emphasize the need of large hosting providers talking more responsibilities.

Consumer organisations strongly call 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.

Online intermediaries call for clear rules and responsibilities that do not disincentivise their proactive actions to limit distribution of illegal content and goods online. In this regard, telecommunication operators highlighted that the paradigm of ‘active’ and ‘passive’ digital services is no longer adequate and need to be clarified. They also call for a duty of care on active hosting providers and proportionate and targeted measures to enable and encourage hosting services providers to take proactive measures.

Several stakeholders, notably new types of services in the internet stack, such as cloud services, CDN and DNS services, other technical infrastructure providers, search engines call for clarifications in the liability regime of intermediaries, without challenging its basic principles.

Telecommunication operators largely agree that some oversight at EU level might be required. According to some, the degree of oversight should vary depending on the services’ obligations and related risks. They also call for improved cooperation among Member States.

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. Some also shared the idea of establishing an independent EU body.

The majority of academia consulted emphasize the need for strong 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. The regulatory oversight must be clear, foreseeable, proportionate, and fair.

National authorities find enforcement as a crucial element to protect users and considers inadequacy of existing cross-border mechanisms and lack of oversight and cooperation between Member States. Some respondents are also in favour of assessing the effectiveness of a European agency and others think that a reinforced cooperation mechanism across national authorities might be sufficient.

5.3. Options discarded at an early stage

The options selection followed a funnelling methodology, exploring the widest spectrum of approaches. Several types of options were discarded earlier in this process, as follows.

Continue 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.

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. 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.

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.

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 through and could 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. Options for changes to general monitoring obligations were considered, and then discarded for non-compliance with the balance of rights described here.

**Lay 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 prone to the same removal obligations as illegal content.

New measures limited to an additional **oversight board**, on top of existing rules. This option would not add significant value, as major issues and gaps in the current system stem from the lack of harmonised rules and the information asymmetries in the digital environment. The option would support to certain extent the cooperation between Member States, but would not address the underlying and the evolving concerns.

6. **WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?**

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

<table>
<thead>
<tr>
<th><strong>Table 3 Summary of impacts for each option considered (compared to the baseline)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Impacts assessed</strong></td>
</tr>
<tr>
<td>Economic impacts</td>
</tr>
<tr>
<td>Functioning of the Internal Market and competition</td>
</tr>
<tr>
<td>Costs and administrative burdens on digital services</td>
</tr>
<tr>
<td>Competitiveness, innovation, and investment</td>
</tr>
<tr>
<td>Costs for public authorities</td>
</tr>
<tr>
<td>Trade, third countries and international relations</td>
</tr>
<tr>
<td>Social impacts</td>
</tr>
<tr>
<td>Enforced and supervision by authorities</td>
</tr>
<tr>
<td>Fundamental and rights (as laid down in the EU Charter)</td>
</tr>
<tr>
<td>Freedom of expression (Art 11)</td>
</tr>
<tr>
<td>Non-discrimination</td>
</tr>
<tr>
<td>Private life and privacy of communications</td>
</tr>
<tr>
<td>Personal data protection (Article 8)</td>
</tr>
</tbody>
</table>
6.1. Economic impacts

6.1.1. Functioning of the internal market and competition

All options considered would have an overall positive effect on the functioning of the single market, but there are notable differences between options. 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.

The second and the third options would in addition reinforce the cornerstone of the single market for all digital services set in the E-Commerce Directive, by clarifying the responsibilities of the country of establishment in supervising services and by clarifying the exceptional conditions under which derogations from the single market principle could be made. It would further establish trust across Member States through an agile cooperation mechanism for cross-border concerns. This would add legal predictability for digital 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 ‘host’ Member States would equally have an effective channel for making sure that the particular challenges of their state are appropriately addressed.

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.

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%\textsuperscript{110}. 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\textsuperscript{111}.

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 captured by requirements, which would be disproportionate for them, while ensuring that certain systemic policy concerns are adequately addressed by very large online platforms. The asymmetric obligations lead to both higher costs on such large platforms, but could also lead to benefits in offering a trustworthy environment 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), assisted by the largest ones, without imposing this as an obligation.
6.1.2. Competitiveness, innovation and investment

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.

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 also 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.

The second and third options would bring stronger improvements to the cooperation mechanisms across Member States and harmonise a wider spectrum of provisions, including online advertising and smart contracts. 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.

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). Complaint and redress mechanisms are important, as set in the Platform to Business Regulation and extended here in all three options, but they do not fully substitute for the premise of a fair and balanced treatment, allowing businesses to rely confidently on their activity on marketplaces. 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.

Overall, the three options would also 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 6.3.1 below). In addition, the legally guaranteed availability of the internal and external redress mechanisms would afford other better protections against erroneous removal and limit losses for legitimate businesses and entrepreneurs.

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.

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. 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.

6.1.3. Costs and administrative burdens on digital services

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.

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 3 Member States.
Compared to projected scenarios where the legal fragmentation would become more acute, the intervention would lead to a save 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 2 Member States.

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.

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.

In addition to these costs, for the second option, services would also incur some technical design and maintenance and reporting cost, for the additional information and transparency obligations presented in paragraph Error! Reference source not found. here-above. 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.

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.

In addition, the third option includes a series of potentially significant costs which are limited to the 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. These costs would vary depending on the initial design of the systems and the ease for extracting data or more robustly modifying systems so that data can be collected and assessed.

SME test

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.

With regard to SMEs offering platform services, since they do not have a scale in their user base equivalent to that of very large online platform, 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\textsuperscript{112}, 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.
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.

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 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.

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.

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 unique users in the Union and of Member States where they are present.

6.1.4. Costs for public authorities

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.

Compared to the baseline, each of the three options should cut significantly the costs brought by the inefficiencies and duplication in the existing set-up for the cooperation of authorities (see driver 2.3.6). In what concerns 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.

With the first option, national authorities would follow a clear, streamlined process for cross-border issues, with clear resolution and response time frames. 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 clearinghouse should significantly improve the ability of Member States to supervise the systemic compliance of services with the requirements.

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 overweight 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.

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 4 Summary of costs for authorities for each option considered

<table>
<thead>
<tr>
<th>Type of activity</th>
<th>Option 1</th>
<th>Option 2</th>
<th>Option 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Supervising systemic compliance with due diligence obligations (country of establishment)</td>
<td>Cost efficiencies: streamline evidence and information for supervising platforms through the clearing house system.</td>
<td>Direct costs: varying from 0.5 FTEs up to 25 FTEs, depending on scale of services hosted</td>
<td>for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.</td>
</tr>
<tr>
<td>2. Law enforcement actions &amp; public authorities requests (re. supervision of illegal activities online)</td>
<td>Cost efficiencies: streamline cooperation processes for cross-border assistance; clear process for information requests to digital services and information obligations</td>
<td>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</td>
<td>for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.</td>
</tr>
<tr>
<td>3. Clearing house</td>
<td>Significant cost efficiencies expected from smoother, clearer cooperation processes</td>
<td>Direct costs: varying from 0.5 FTEs up to 25 FTEs, depending on scale of services hosted</td>
<td>for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.</td>
</tr>
<tr>
<td>a. Country of establishment</td>
<td>0.5FTE per 5K requests per year (expected to be lower for most MS, and increase per requests should not be linear)</td>
<td>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</td>
<td>for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.</td>
</tr>
<tr>
<td>b. Host country</td>
<td>0.5FTE per 5K requests issued per year (expected to be lower for most MS, and increase per requests should not be linear)</td>
<td>One-off: ~ 15 FTE for setting up and maintaining a shared database and cooperation tools (over 2 years)</td>
<td>for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.</td>
</tr>
<tr>
<td>c. EU-level: for clearing house and coordination</td>
<td>One-off: ~ 15 FTE for setting up and maintaining a shared database and cooperation tools (over 2 years)</td>
<td>Recurrent: 1 FTE for running the system, and technical analysis + computing costs for servers (absorbed in EC IT infrastructure)</td>
<td>for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.</td>
</tr>
<tr>
<td>4. Supervision of enhanced obligations for online platforms – expenditures at MS level and/or EU capability</td>
<td>Significant cost efficiencies through enhanced transparency obligations on platforms</td>
<td>Costs expected to fluctuate depending on inspections launched. For one inspection/audit, estimates between EUR 50 K and EUR 300K.</td>
<td>for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.</td>
</tr>
<tr>
<td></td>
<td>Costs expected to fluctuate depending on inspections launched. For one inspection/audit, estimates between EUR 50 K and EUR 300K.</td>
<td>Codes of conduct and co-regulatory framework: investment at EU level of 0.5-2 FTEs per initiative</td>
<td>for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.</td>
</tr>
<tr>
<td>5. EU Board</td>
<td>EU level: 25 FTEs</td>
<td>Participation from each MS: 0.5 FTE</td>
<td>for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms.</td>
</tr>
</tbody>
</table>

6.2. Trade, third countries and international relations

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.

They would require a legal representative in the Union. This is not expected to have a significant effect on legitimate platforms from third countries targeting the single market. For most of them, it is likely that legal representatives are already established as part of other legal requirements under EU legislation (e.g. General Data Protection Regulation (‘GDPR’)115) and would absorb to a
large extent this cost. In addition, compliance with EU rules could be a commercially beneficial trust signal for such providers.

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 – not least 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.

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 a 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. However, the options, and in particular Option 3, will be carefully considered and designed in a manner that is compliant with the EU’s international obligations for market access and non-discrimination, in particular the measures designed will be specific and clear to fulfil key policy objectives to provide a safe online environment contributing to public order and protection of consumers.

### 6.3. Social impacts

#### 6.3.1. Online safety

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.

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 persons.

The second and the third options 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. The two options would in addition 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.

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.

The third option, however, would include a much stronger accountability mechanism, 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.

As the COVID-19 crisis has shown, crisis situations present systemic risks and require coordinated interventions; the third option would also include a framework for establishing such cooperation in crisis situations, together with the appropriate checks and balances for both platforms and authorities.

6.3.2. Enforcement and supervision by authorities

A first notable impact, already explained in section 6.3.1, is the improved ability of law enforcement and authorities to supervise and tackle online crimes.

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 dissuasive sanctions for systematic non-compliance with the due diligence obligations. However, 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.

Importantly, the second and the third option each harmonise conditions for court and administrative orders requesting removal of individual or identical content. This should facilitate the actions of the authorities and lead to better enforcement overall.

In addition, the second option gives in addition 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.

Finally, with regard to the effective supervision of all digital services in the single market, as clarified in section 6.1.1, in particular paragraph 173 above, there are notable differences between the first, second and third options.

6.4. Impacts on fundamental rights

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.116

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 their ability to continue to offer a ‘future proof’ due process faced with the evolving risks emerging in a highly dynamic digital environment.
All three options would also include a requirement to companies to adopt a ‘fundamental rights by design’ approach 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.

Where option 3 sets a framework for co-regulatory measures, the requirement for respecting fundamental rights by design will 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.

The fundamental rights most clearly touched upon by the intervention are as follows:

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

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.

Neither of the options includes prior authorisations 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

All three options would add substantial improvements to the baseline situation, by imposing mandatory safeguards when users’ content is removed: 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.

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’\(^\text{117}\). 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.\(^\text{118}\)

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.

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. 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. 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 chilling effects on speech

Some evidence shows that highly violent online environments, for example, have to 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. All options would empower users to report illegal content and support a safer online environment (see section 6.3.1 above).

c. Stimulating freedom to receive information and hold opinions

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 at paragraphs 225 to 227 here above. In fostering exchanges of information, this can also have spill-overs on users’ freedom of assembly and association.

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 to democratic processes or consumers to make informed choices. The third option would establish a higher standard of accountability 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.

6.4.2. User redress

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.

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.

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.

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.

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

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, affecting them with prominence. In this regard, each option would have different strengths of impact, as assessed in section 6.3.1 above (Online safety).

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 options 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.

The three options would address the risks by affording safeguards aimed at improving the possibility for contesting such restrictions (as per 6.4.2). 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.

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.

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.

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

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.

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

For all three options, obligations to set up a ‘Know Your Business Customer’ policy and collect identification information from business users, as well as obligations to for the identification of advertisers would likely imply the collection of personal data.
Similarly, where option 3 requires further reporting to national authorities, this can entail disclosure of personal data of business 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 professional users conducting commercial transactions through the online intermediary (e.g. selling goods, offering services, buying ad space). It does not cover in any way requirements for citizens using online services to identify themselves. The requirement would offer a legal basis for data processing in line with Article 6 (1) c) of the GDPR, would apply fully the data minimisation principle, and would require Member States to specify the conditions for data processing by the requesting authorities, as required by Article 6 (3) of the GDPR.

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.

**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.

As regards risks posed by automated content moderation and other technologies voluntarily used by platforms for tackling illegal behaviours of their users – see paragraph 237 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. None of the three options would affect in any way this requirement. Option 3 would instead potentially create additional opportunities for inspecting compliance in this regard.

**6.4.5. Rights of the child (Art 24 of the Charter)**

All three options would have a positive influence in protecting the safety of children online – see section 6.3.1).

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

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

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.

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.
6.5. Environmental impacts

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.

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.

In addition, many illegal activities are also related to intense polluting – see, in particular, the case of counterfeit products\textsuperscript{121} 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\textsuperscript{122}.

7. HOW DO THE OPTIONS COMPARE?

7.1. Criteria for comparison

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

- **Effectiveness in achieving the specific objectives:**
  
  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\textsuperscript{123}

- **Proportionality:** whether the options go beyond what is a necessary intervention at EU level in achieving the objectives

7.2. Summary of the comparison

Summary of the comparison of options against the four criteria is included below. See also detailed comparison on specific impacts presented in section 6, paragraph 172 above. Table comparison of options should only be read in vertical:
7.2.1. **Effectiveness**

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

The first option would improve 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. This would answer to the most acute and current concerns Member States are raising at this point in time and improve 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. However, it would not be effective in the medium to long term in establishing the flexible and responsive framework to address emerging issues or problems posed by other digital services.

The second option would significantly improve the effectiveness of the intervention by providing better legal certainty to all online intermediaries, not just online platforms and by re-establishing trust between Member States authorities through a reinforced and more agile cooperation mechanism addressing current and emerging issues related to digital services.

The third option would be the most effective in establishing the best conditions for all digital services to develop 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 would 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 also would calibrate these efforts and target them towards those services producing the biggest impacts. 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**

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.

The second option would be expected to produce stronger 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. recommender systems or ads they see.
The third option would be most effective in achieving the objective. In addition to the features of option 2, it would include stronger obligations and significantly more robust oversight on very large online platforms. It would also create a flexible co-regulatory environment to address in an adapted and speedy manner all emerging issues, ensuring 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.

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

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.

The second option would be significantly more effective, giving 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.

The third option would be the most effective in this regard, complementing measures empowering users with oversight and supervisory powers 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

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

The second option would significantly 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.

The third option would offer the most 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 affording the appropriate oversight powers to authorities and facility access to information to researchers ensuring that issues can be detected as they emerge.

7.2.2. Efficiency

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

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.

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.

The third option is similarly costly for all digital services, but requires higher compliance costs from 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. This option is consistently more effective than the others, in
particular in addressing complex information asymmetries and issues expected to emerge in the future.

7.2.3. Coherence

7.2.3.1. Within the Digital Services Act Package

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

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.

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 in the second instrument. 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 and their presence across Member States (see paragraph 161).

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

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.

They would also provide for an effective cooperation and supervision system, with different degrees of impacts (see 6.1.1 and 6.3.2) which could further support sector-specific cooperation.

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).

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

All three options are fully aligned and reinforce the principles of the open internet and the technical infrastructure of the network. Option 3, in particular, further clarifies the liability exemption for key services in the internet stack. 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

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

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 established 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.

It would also appropriately manage systemic risks which emerge on very large platforms, while establishing a level playing field for smaller players – both 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.

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:

<table>
<thead>
<tr>
<th>ALL ISS</th>
<th>ALL INTERMEDIARIES</th>
<th>ONLINE PLATFORMS</th>
<th>VERY LARGE PLATFORMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information requirements</td>
<td>General disclosure rules on advertising</td>
<td>Fundamental rights by design</td>
<td>Transparency reporting obligations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transparency reporting obligations</td>
<td>Transparency reporting obligations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Notice and action</td>
<td>Notice and action</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trusted flaggers</td>
<td>Trusted flaggers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Penalties for abusive notices and counter-notices</td>
<td>Penalties for abusive notices and counter-notices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certified dispute resolution bodies</td>
<td>Certified dispute resolution bodies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transparency of (algorithmic) content moderation practices</td>
<td>Transparency of (algorithmic) content moderation practices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vetting credentials of third party suppliers (“KYBC”)</td>
<td>Vetting credentials of third party suppliers (“KYBC”)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Codes of conduct</td>
<td>Codes of conduct</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transparency of recommender systems and user choice for access to information</td>
<td>Transparency of recommender systems and user choice for access to information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data sharing with authorities and researchers</td>
<td>Data sharing with authorities and researchers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External risk auditing and public accountability</td>
<td>External risk auditing and public accountability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Crisis response cooperation</td>
<td>Crisis response cooperation</td>
</tr>
</tbody>
</table>
9. **REFIT (Simplification and Improved Efficiency)**

Table 6 REFIT cost savings for the preferred option

<table>
<thead>
<tr>
<th>Description</th>
<th>Amount</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coordination and cross-border cooperation costs for national authorities will be significantly streamlined through the Clearinghouse system and the EU body</td>
<td>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</td>
<td>Concerns mostly national authorities in Member States</td>
</tr>
<tr>
<td>Core elements of the harmonising measures: due diligence obligations for online intermediaries</td>
<td>Between EUR 400.000 and EUR 15 mil for a medium-sized company, per year</td>
<td>Concerns hosting service providers, in particular online platform companies established in the Union</td>
</tr>
</tbody>
</table>

10. **How will actual impacts be monitored and evaluated?**

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.

Several monitoring actions should be carried out by the Commission, in evaluating continuously the effectiveness and efficiency of the measures. However, quantitative indicators are not set here as key performance indicators, as the framework is designed to adapt to the dynamic challenges of the digital world.

Table 7 Summary of monitoring actions and indicators

<table>
<thead>
<tr>
<th>Specific objectives</th>
<th>Operational objectives</th>
<th>Monitoring and indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Best conditions for innovative cross-border digital services to develop</strong></td>
<td>Harmonised application of due diligence obligations for online platforms</td>
<td>Monitored through the reported data from the Clearinghouse system, with qualitative indicators based on requests for assistance from MS, response rates and resolutions. Reports from MS through the cooperation of the EU Board</td>
</tr>
<tr>
<td></td>
<td>Legal certainty and consistency in</td>
<td>Monitoring of the evolution of CJEU case law,</td>
</tr>
<tr>
<td>2. <strong>Safe online environment, with responsible and accountable behaviour from digital services</strong></td>
<td>enforcement with regard to the due diligence obligations and the legal clarity in the liability regime for online intermediaries</td>
<td>national case law and complaints resolved in out of court dispute resolution mandated by the act.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>Mitigate and prevent further burdensome legal fragmentation for digital services</td>
<td>Infringements launched against Member States (numbers and diversity of infringements and services concerned)</td>
</tr>
<tr>
<td></td>
<td>Effective application of the due diligence obligations by service providers</td>
<td>Continuous monitoring of laws reported by Member States restricting information society services. Monitoring requests for guidance and issuing of guidance by the EU Board</td>
</tr>
<tr>
<td></td>
<td>Effective actions by law enforcement</td>
<td>Monitoring co-regulatory frameworks launched under the requirements of the act, their reported outcomes and the extent to which they address the underlying concerns and cover all relevant digital services and social partners.</td>
</tr>
<tr>
<td>3. <strong>Empower users and protect fundamental rights online</strong></td>
<td>Compliance from service providers with due diligence and transparency obligations</td>
<td>Data reported by Member States supervising the systemic compliance of service providers – as collected through the Clearinghouse Number, complexity and effectiveness of cases pursued by the EU Body</td>
</tr>
<tr>
<td></td>
<td>Investigations, audits and data requests from authorities, researchers and independent auditors</td>
<td>EU Body enforcement measures and technical investigations launched</td>
</tr>
<tr>
<td></td>
<td>Effective supervision and enforcement by Member State of establishment</td>
<td>Monitoring of transparency reports, ad archives and compliance with specific requests from authorities and independent audits of service providers</td>
</tr>
<tr>
<td>4. <strong>Appropriate supervision of digital services and cooperation between authorities</strong></td>
<td>Responsive and effective cross-border cooperation</td>
<td>Monitored through the reported data from the Clearinghouse system, with qualitative indications based on requests for assistance from MS, response rates and resolutions. Reports from MS through the cooperation of the EU Board</td>
</tr>
</tbody>
</table>

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.

Instead, the effectiveness of the instrument is likely to be strictly dependant 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. A review of the intervention should be planned, in this regard, five years after entry into force.
ENDNOTES

3 See Annex 5 for details about the evaluation of the E-Commerce Directive.
8 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.
9 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 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
10 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, 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.
11 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
12 from optimisations through network technologies to development of artificial intelligence applications or blockchain technology and distributed data processing.
13 40% in 2019 in EU27, according to ESTAT https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do See also (Eurobarometer - TNS, 2016) for more granular data based on a 2016 survey
14 Duch-Brown & Martens, 2015
15 Iacob & Simonelli, 2020
16 (Eurobarometer - TNS, 2018)
17 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/).
21 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,
22 (OECD/EUIPO, 2019)
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 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.

By contrast with the EU definition (see endnote Error! Bookmark not defined.), 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.’

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

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

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


See, for example, potential trade-offs and welfare losses in using alternatively recommender systems and targeted advertising as marketing strategies in (Iusi Li, 2016)

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

For example (Jausch, 2020) or (Fundacja Panoptykon, 2020)

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

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

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.

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


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-
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](https://netflixtechblog.com/netflix-recommendations-beyond-the-5-stars-part-2-d9b96aa399f5)


On the need for continuous, structural monitoring, see e.g. (LNE, forthcoming) (Urban, 2017)


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


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

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)

(Eurobarometer - TNS, 2018) (Penney, 2019) (Matias, 2020)

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

Simulated based expenditure data from publicly available reports from companies complying with the requirements in the NetzDG. See Annex 4

Conservative estimates based on data available in the Dealroom database for ‘hosting services’ having received some venture funding or other external investment (September 2020)

See annex 4 for an explanation of the model


(Eurobarometer - TNS, 2018) (European Commission, 2020)

Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online

Most prominently, [https://www.oversightboard.com/](https://www.oversightboard.com/)


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/](https://ecommercenews.eu/amazon-has-1-1-million-active-sellers-in-europe/)

Data extracted from similarweb, computing average number of users in 2019

Statista, based on IHS and IAB Europe data


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


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


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

Tackling Illegal Content Online Towards an enhanced responsibility of online platforms (COM/2017/0555 final)


See annex 12 for a more detailed description fo EU law framing online advertising


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


See the Evaluation report in Annex 5

In C-484/14, McFadden, the Court interpreted that wifi-hotspots are covered by Article 12 ECD. Less conclusively, in C-521/17, SNB-REACT the Court interpreted that IP address rental and registration services (DNS registrars) may be covered by Articles 12 to 14 ECD, depending on the circumstances. In C-236/08, Google France the Court determined that Google as referencing service provider could be covered by Article 14 ECD.

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“

In case C-682/18 YouTube.

The relevant provisions have been recently interpreted by the Court, who has confirmed that a Member State’s failure to fulfill 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.

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)

2019 Survey, 2020 targeted questionnaire, discussion in the e-Commerce Expert Group in October 2019

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)

See Annex 4
Using as benchmark private sector estimates of online cross-border trade
second-edition-of-the-top-500-cross-border-retail-europe-an-annual-ranking-of-the-best-500-european-
cross-border-online-shops/

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 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.

Large online platforms.

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

(LNE, forthcoming)

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

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

Cases C-70/10 (SABAM v Scarlet) and C 360/10 (SABAM v Netlog NV)

See Annex 11

United Nations Special Rapporteur on violence against women, thematic report on violence against

processing of personal data and the protection of privacy in the electronic communications sector

(European Commission, 2020)


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