PromethEUs

PromethEUs Paper, June 2021

PromethEUs Paper

TOWARDS A NEW EUROPEAN DIGITAL ENVIRONMENT

Preparing for the DSA and DMA revolution

Executive Summary

The growth of the **digital sector** has led to the rapid development of multiple services that cover a wide range of daily activities. As well as the clear and huge benefits, several challenges, mostly either unknown or overlooked at the dawn of the Internet, have arisen from its ever growing popularity. After several interventions, mostly sectoral or more limited in scope and scale, on 15 December 2020, the European Commission published a double proposal for a Regulation on a Digital Markets Act (**DMA**) and a Regulation on a Single Market for Digital Services (**DSA**). The former deals with the identification of different responsibilities in the offer of services, while the latter concerns the economic imbalances and unfair business practices by the so-called "gatekeepers". The main challenge of the regulatory framework is to avoid penalising the **high rate of innovation and dynamism** that characterise this sector. Moreover, there are peculiarities specific to the digital market that authorities need to take into consideration, such as network effects, the large use of user engagement strategies and the huge amount of data involved in the supply of digital services.

Chapter 1 examines different digital market segments in order to identify the main characteristics, specific features and common trends, as well as attempting to understand if clear boundaries can effectively be identified between different market segments. The analysis points out how the last twenty years have been marked by the **growing success of digital services in most sectors of the world economy**. If this has led to the growth of web giants with important market quotas, at the same time, it should not be overlooked that they have also been **significantly contributing to the dynamic evolution of the tech world.** They have fostered rapid development and innovation, increasing market efficiency, facilitating trade, and ensuring overall sizeable benefits for citizens, businesses and public administrations alike. These trends have made it increasingly clear that digital technologies are an indispensable part of the economy and, at the same time, that they need to be regulated within a comprehensive and consistent EU-wide normative framework. **As well, the heterogeneity and fluidity of the digital markets make it difficult to apply clear cut definitions** to services provided by different platforms. With **market boundaries becoming increasingly less defined** and traditional markets now being taken over by **technological disruptions**, digital markets

have become radically different to those businesses, scholars and regulators had been accustomed to.

The impressive level of dynamism, together with the ability of new players to achieve prominent market positions within a few years, are elements of great contrast and change compared to what had characterised the 'traditional' markets for decades. A global perspective taking into account the **speed that technology is affecting the deployment of new services and market dominance** is required in order to **define market dynamics, the degree of competition and the scalability opportunities arising in each of the different sectors of the digital economy**.

Where **e-commerce** is concerned, in 2019, services linked to online shopping accounted for 20% of the turnover of European companies due to the shift of many businesses to digital platforms driven by the need to reach a larger number of customers at lower costs. Moreover, the global pandemic has further accelerated e-commerce development pushing up the forecast on total European e-commerce turnover to exceed $500 billion by 2024. Nowadays, 76.8% of the global population shop online in a month, however, the contribution of e-commerce to GDP is still limited: only in China does its share exceed 10%. The main digital platform in Europe is Amazon with 1.1 billion visits per month, but competition is rife with other actors, such as the American eBay, the German Zalando, the British Asos and the French PriceMinister. On the other hand, the American market seems to be less fragmented, as Amazon and eBay alone account for almost 80% of the market.

The importance of the **operating system and app-store** segment is highlighted by the fact that two thirds of the global population own a smartphone and that, in January 2021, Google Android users spent on average 4 hours per day on their mobile devices. Smartphones are now indispensable tools in the daily lives of millions of people and, while the market for mobile phone hardware is still competitive, the market for enabling software is currently led by the duopoly of Google Android and iOS, together accounting for 99% of the market. However, while the former is more widely spread in different parts of the world, probably because of its open-source nature, the latter is the market leader in the US and Japan. At the same time, as further proof of the complexity and dynamism of these markets, it is interesting to note how the HarmonyOS project, launched in 2019 by Huawei, could seriously undermine, at least for non-US markets, the current market equilibrium that has been reached in recent years at global level.

When it comes to **social networks**, services would need an in-depth individual analysis as it is extremely hard to identify the clear boundaries and distinctions between them. This sector may include traditional networking services, instant messaging apps, streaming and content sharing platforms and so on. The economic value of such platforms depends on the number of users they can attract as their turnover is closely linked with advertising services that may rely on the huge amount of data they can gather. By the end of 2021, the number of social media users will be closer to 4.9 billion and will involve 48% of the European population. An interesting trend sees end-users beginning to use the social network as search engines as 45% of Internet users claim to access social

networks at least once a month when searching for information on products or services they are considering to purchase.

Other important segments of the digital market are **search and ads**. General search services allow consumers to collect information by entering any keyword in a search engine platform, which then uses algorithms to evaluate the relevance of information on all publicly available webpages. The search engine delivers results within a few seconds and also includes ads in various forms. These services are funded by ads and so the collection of users' personal information and preferences is key, as well as the possibility to fully take advantage of economies of scale that allow for the use of AI learning algorithms using massive data bases. Even if the global market structure is very concentrated, technological trends challenge incumbents, such as the spread of non-conventional search methods - voice search technologies, the use of social media platforms for commercial information search, and the use of image recognition tools on mobile devices. The market is shifting from desktop to mobile services, making future developments harder to predict. The channels used are multiple, and involve search, social media, banner, video and other means.

Cloud computing is an environment that provides networks and access to computing resources. It is made up of two components - hardware infrastructure and software applications. Its purpose is not to spread information but, instead, to offer a secure environment to store personal data, that is only used by owners. It is worth noting that 70% of the market share is in the hands of the top 8 providers (the so-called "hyperscalers", with the global scale, expertise, cutting-edge innovation and broad range of services needed to maximise cloud value[1]). The global cloud computing market is increasing both in value and strategic importance, and by 2025, it is expected to reach $832.1 billion in revenues. Several EU Member States have started to deploy an autonomy strategy in order to counteract or at least regulate the trend that sees European companies and public administrations relying on non-European providers. Where this is concerned, as the purpose of the cloud is not to disseminate information on a large scale, but rather to offer a secure space in which users can store their personal data, forcing a control over user data does not seem an appropriate measure considering its technical characteristics and business model, and would risk jeopardising user privacy, thus, resulting in the cloud losing one of its main competitive advantages.

Chapter 2 deals with the **spread of illegal and harmful content online**. As already mentioned, digitisation has created incredible new economic opportunities and improved the quality of life of individuals, but has also raised some critical issues. Web users are exposed to increasing risks due to the spread of illegal activities, the infringement of fundamental rights and other societal harm. Online illegal activities include the dissemination of illegal content, illegal marketing services and the sale of illegal goods.

In this scenario, online platforms today play a key role in distributing and shaping information online, assuming a responsibility that, although not definable in typical editorial terms, seems to

[1] Accenture (2020), *Hyperscale your cloud journey: Partner for more value*.

extend far beyond the mere technological aspects. To stem this spreading of harmful content and protect their users, organisations carry out careful monitoring of published content.

One of the most serious problems on the Internet is the spread of **fake news**. The **fight against disinformation** is a major challenge for Europe and poses a threat to the future of democracy. According to the latest data of Eurobarometer, 71% of Europeans encounter fake news online several times a month (30% every day). Those who seem to be most exposed are young people who, in 63% of the cases, say they come into contact with fake news at least once a week.

In order to face this potential threat, the European Commission published a **Communication on Tackling Online Disinformation** in April 2018, followed by the **"Code of Practice on Disinformation"**, the first worldwide self-regulatory set of standards to fight disinformation. This was voluntarily signed by digital platforms, leading social networks and advertising industry. This measure proved to be fundamental in the fight against the spread of false news during the Covid-19 pandemic. Indeed, since the outbreak of the pandemic, operators have blocked millions of harmful content related to this issue.

In May 2021, the European Commission published its **guidance on how the Code of Practice on Disinformation should be strengthened** to become an even more effective tool for countering disinformation. It sets out Commission expectations, calls for stronger commitments by the signatories and foresees a broader participation in the Code. According to the Commission, signatories should reduce financial incentives for disinformation, empower users to take an active role in preventing its spread, cooperate better with fact-checkers across different EU Member States and languages and provide a framework for researchers to access data. Some of these issues are already embedded in the DSA proposals, published by the Commission in December 2020.

Another very serious problem is related to the online dissemination of content concerning **hate speech, terrorism and paedophilia**. The main difficulties concerning hate content concern striking the right balance between protecting people and ensuring freedom of speech. Here, it is worth noting how the transnational nature of the Internet makes it difficult to set universal limits or boundaries.

In 2016, several tech operators jointly agreed to a **European Union Code, voluntarily assuming the responsibility to review the "majority of valid notifications for removal of illegal hate speech" uploaded on their services within 24 hours**. On 22 June 2020, the European Commission released the results of its fifth evaluation of the Code, finding that, on average, 90% of flagged content was assessed by the platforms within 24 hours, while 71% of the content deemed to be illegal hate speech was removed in 2020 (compared to only 28% in 2016). Currently, according to the review, platforms continue to respect freedom of expression and avoid removing content that may not qualify as illegal hate speech.

Looking at the numbers, thousands of hate content uploads appear on various web platforms every day. Data disseminated by Facebook on **blocked malicious content** shows that, in the last quarter only, the social network acted against over 25 million hate content uploads. Unfortunately, the

trend is increasing and, between the first quarter of last year and the same period of this year, the hate content removed has almost tripled (+165%). The social network has to also deal with a huge amount of **content flagged as terrorist**. According to the latest data published, in the first quarter of 2021, Facebook blocked approximately 9 million terrorist messages. Similar issues were faced by Twitter which, in the first half of 2020, acted against 635 thousand accounts and almost 1 million in content flagged as hateful conduct. To provide an idea of the proportions, they accounted for about 50% of the total content removed for violating platform rules.

Besides dealing with harmful content, platforms also play a key role in preventing **unfair business practices**. This already widespread problem has been further intensified by the pandemic. For instance, rogue traders began advertising and selling products such as protective masks, caps and hand sanitisers that could allegedly prevent infection.

The Commissioner for Justice and Consumers, Didier Reynders, wrote to the main digital players (social media, search engines and market places) in order to request their **cooperation in tackling and taking down scams from their platforms**. The numbers provided by Twitter, Google and Microsoft give ad idea of the magnitude of this problem. During the pandemic period Twitter identified 11,307 ads promoting unacceptable business practices, while the total number of violations of Google Ad accounts was 314,286. The EU country with the highest number of recorded violations was Italy (37,694), followed by Germany (28,267) and France (26,466). The same trend was registered by Microsoft, as, in 2018, its Microsoft Advertising service suspended nearly 200,000 accounts and removed 900 million bad ads and 300,000 bad sites.

Even the number of **scams and counterfeiting goods purchased by e-commerce users** has significantly increased as a consequence of the pandemic, forcing customers not used to online services to the web, making them an easy target for malfeasants. Hence, companies now must deal with adopting strategies to balance the trade-off between a frictionless purchasing experience for the customer and highly reliable protection systems. Still, the **cost of fraud** in terms of revenue losses and clients abandoning the service cannot be underestimated. In this perspective, consumer protection strategy design is shifting from a defensive to a business optimisation approach, also because as a large amount of data is involved, machine learning technologies are required to be used together with human investigation and monitoring.

Chapter 3 presents the new regulatory framework in digital services. The digital revolution, accelerated by the pandemic resulting in a massive use of digital services to ensure the continuity of social and economic activities and guarantee fundamental rights and freedom, has called for a rethinking of the role and responsibilities of platforms and, therefore, of the relevant regulatory framework. To this end, on 15 December 2020, the European Commission published a package of two legislative initiatives - the Digital Services Act (DSA) and the Digital Markets Act (DMA). In order to promote a maximum harmonisation in the EU and, thus, overcome the current regulatory fragmentation, the Commission has opted for directly applicable regulations instead of directives.
The **DSA** amends, while maintaining its key principles, the E-commerce Directive (Directive 2000/31/EC), in order to ensure the best conditions for the provision of innovative digital services

in the internal market, to contribute to online safety and the protection of fundamental rights (above all, freedom of expression and information) and to establish a sound and sustainable governance model for the supervision of intermediary service providers. The proposal, following a public consultation, is divided into five chapters, introducing a **horizontal framework** for all categories of content, products, services and activities on intermediation services. However, for the latter, a **diversified liability regime** has been outlined on the basis of the services offered and the size of the supplier and **specific obligations for the Member States** have been set to verify the compliance of these subjects operating in their respective territories with respect to the provisions contained in the proposed regulation. As well, **new subjects** (Coordinators for Digital Services) have been established and **mechanisms of enforcement and cooperation** between Member States defined.

The **DMA**, instead, is concerned with economic imbalances, unfair business practices by gatekeepers and their negative consequences. It aims to ensure the contestability of digital markets, a fair B2B and B2C relationship between market gatekeepers and their users and to strengthen the internal market by providing harmonised rules across the Union. The proposal establishes a series of strictly defined **objective criteria** to qualify a large online platform as a gatekeeper and, according to an ex-ante approach, sets a series of **obligations and prohibitions** on these subjects. The proposed regulation also defines in detail the **powers of the Commission**, granting it the power to request information, conduct inspections, order interim measures, make binding commitments proposed by the gatekeeper, carry out monitoring activities regarding compliance with the obligations under the proposed regulation, adopt decisions certifying infringements by gatekeepers and impose **penalties**. The latter are quantified up to 10% of the total annual worldwide turnover of the company (and periodic penalty payments of up to 5% of the average daily turnover). Moreover, as a last resort, systematic violation of the regulations may lead to the application of extraordinary structural remedies such as the obligation to sell part of the company's assets or property.

Chapter 4 investigates the economic impact of the DSA package in terms of three main dimensions: **a) the impact on businesses, focusing on SMEs, b) changes in competition in the Digital Single Market, and c) the effect on competitiveness and innovation**. Most firms are reshaping and digitalising many of their activities. Online markets are quickly emerging as the primary source of firm revenue. EU performance regarding business digitalisation and e-commerce has improved over the last five years. The COVID-19 pandemic has amplified the importance of digitalisation and created new opportunities for businesses to retain their market position and resilience. The emergence of digital markets is fertile ground providing opportunities for new business ventures and the expansion of already established actors. Focusing on SMEs, the dominant type of firm in the EU (approximately 99% of all enterprises), a new single EU digital market could foster a wave of positive spillovers.

Furthermore, legal fragmentation across Member States is a critical issue hindering the optimal functioning of the Single Market. The DSA aims to support cross-border sales by decreasing the costs of operating where possibly 27 different business regimes are involved, since complying with diverse regulatory and administrative requirements is challenging for growing businesses, especially where cross-border business is concerned. Up to now, expanding into foreign markets has been a venture that predominantly only the larger enterprises have undertaken. SMEs were and still are in a rather disadvantageous position compared to their larger counterparts. Hence, the facilitation of an EU Single Market is essential for improving overall performance in EU digital markets.

Nevertheless, **the proposed regulation carries many entrepreneurial challenges and risks.** Creating a heavily regulated environment that strains economic activity instead of promoting it is a credible hazard. Even though the DSA's initial approach establishes a more harmonised environment, the differences in Member State legislative systems create a further burden for businesses, especially SMEs. There is an overlapping of this new instrument with the national equivalents. The definition of several terms, such as the very large platforms, users, the good Samaritan clause, illegal content, need to be further clarified, as they seem to be rather vague concepts. The inclusion of harmful content could have an additional negative influence since it increases the ambiguity of the legal framework. The extent of the regulations and their implications could significantly distort the efficiency of the digital markets. The lack of explicit legal definitions that rely on interpretation is currently deterring firms – particularly SMEs - from entering new markets and operating efficiently.

Potential over-regulation of platform activities could lead to missed business opportunities. Flexibility is critical for business users so they can embark on economic endeavours that may otherwise be lost. Efficient enforcement of ex-ante rules requires predictable parameters and operators should be able to anticipate as much as possible whether they will be subject to the rules. The additional identification, concerning the new "Know your customer" (KYC) obligations, could place an extra burden on the platforms since more information and procedures would be required by registered users decreasing the pace in attracting new users.

Moreover, the lack of authority involvement in the consumer flagging procedure is worth further investigation since it could lead to negative behaviour causing problems for a firm's optimal functioning.

Considering the above-mentioned factors, **the final impact on SMEs calls for a further examination**. **The right balance must be found between decreasing the existing administrative burdens in doing business across Europe and imposing new invisible obstacles for SME potential growth**.

The new legal framework is essential for regulating digital competition, which has greatly changed over the years. Instead of a specific product-market, systems of complimentary services have emerged that attract both intermediate and end consumers. The frontier between digital and non-digital space has become blurred, and updating the legal framework seems to be imperative. The

objective of the DSA/DMA is to ensure contestable and fair markets in the digital sector. Still, fairness is a relatively new thing to competition law. **Over-regulation appears to be a credible hazard that could result in unforeseen spillovers. Combining a vague legal framework and severe restrictions for large platforms could lead to an over-reaction on the part of the big players.** With a threat of harsh penalties, large platforms could exaggerate their activities and overly limit the displayed content compared to the social optimum. Platforms, and especially search engines, not only provide specific content to users, but they are also responsible for its prominence, a critical aspect that seems to have been neglected. Interference in this could not only bring about a significant distortion in competition, but also limitations on exercising fundamental rights.

Moreover, it is common knowledge that an over-regulated market kills innovation as it greatly hinders any new efforts. The facilitation of doing business is a key factor for encouraging innovative activities, international research collaborations and technology developments. The positive relationship of regulatory costs to a player's size allows new players to stay small, otherwise, their costs would dramatically rise. Last but not least, digital foreign direct investment and trade could be deterred since the new legal framework would add undue costs on operating in Europe. A heavily regulated environment is a serious disadvantage for European international competitiveness, while the contribution of digital trade to economic growth has become greater than ever.

Finally, the digital gap between the North and South of Europe should be taken into consideration. The EU must bridge this gap as soon as possible where a common legislation is vital for technological advancement and innovation growth.

In the **conclusions,** it is recalled that the DSA and DMA proposals will bring about important changes, redesigning the role and responsibilities of platforms and producing a strong impact on them and on the market. For that reason, a careful analysis of the effects of the specific norms is essential.

As regards the DSA proposal, an **adequate balance is required** between the necessity to guarantee rights and freedom and the opportunity not to hinder, but rather foster, innovation and competitiveness in the European Union through the introduction of an **over-regulated system**. To this end, in general, a **clear and transparent regulatory framework** must be drawn up, ensuring coherence and avoiding the duplication of the obligations stemming from the DSA and from other texts such as the Platform-to-Business Regulation and the Copyright Directive. In discussing the obligations placed on the platforms, **achievable and proportionate obligations** should be set. This is also in consideration of the impact of **compliance costs** on small players and to avoid the risk that a regime too focused on large platforms may favour the displacement of illegal activities and content to smaller platforms, which are less equipped to deal with them.

Moreover, if the principle that everything that is illegal offline should be illegal online seems sound (though with some limitations due to different technologies and contexts), the opposite should also hold true (for instance, for self-preferencing and advertising). However, the DMA (and partially the

DSA) could create **an artificial barrier, not only between digital and physical ecosystems, but also between digital and physical companies while the path is always towards convergence**. Higher standards for digital intermediaries and platforms than for physical entities may slow down the digitalisation of traditional companies and market contestability.

Another means to increase market contestability, creating significant innovation and efficiency gains, is by **allowing gatekeepers to compete with each other**. However, art. 5 and 6 in the DMA regulations would obstruct this possibility (that represents how innovation works in many instances, along with the other possibility of startups emerging against big players).

Parliamentary Reports and **the non-paper by the governments of France, Germany and the Netherlands on the DMA**, while appropriate and sensible in many cases, raise some serious doubts that need to be addressed. These involve the risks of interference in fundamental principles, limitations on the development and use of technology, fragmentation of the internal market and adverse effects on SMEs.

CONTRIBUTORS

Introduction, Chapters I, II & III – I-Com

Stefano da Empoli
Silvia Compagnucci
Lorenzo Principali
Domenico Salerno
Thomas Osborn
Giorgia Pelagalli

Chapter IV – IOBE
Foundation for Economics & Industrial Research

Aggelos Tsakanikas
Maria-Theano Tagaraki

**This joint paper has been developed by I-Com, Institute for Competitiveness (Italy), and IOBE - Foundation for Economic and Industrial Research (Greece).*

Introduction

Digital services have brought about important innovative benefits for users and contributed to the internal market by opening up new business opportunities and facilitating cross-border trading. These digital services cover a wide range of daily activities including online intermediation services, such as online marketplaces, online social networking services, online search engines, operating systems or software application stores increasing consumer choice, improving industry efficiency and competitiveness and facilitating communication amongst people, as well as freedom of speech and civil participation in society.

Along with the clear and enormous benefits, several challenges, mostly either unknown or overlooked at the dawn of the Internet, have arisen from its popularity. After several interventions, mostly sectoral or more limited in scope and scale, on 15 December 2020, the European Commission published a double proposal for a Regulation on the Digital Markets Act (DMA) and a Regulation on a Single Market for Digital Services (DSA) that are the result of two wide-ranging public consultations.

The DSA introduces a system of diversified responsibilities based on the services offered and the size of the provider, places specific obligations on Member States to verify the compliance of those entities operating in their respective territories with the provisions contained in the proposed regulation. It also sets up new entities (Digital Service Coordinators), and defines enforcement and cooperation mechanisms between Member States to better protect consumers, ensure the exercising of their fundamental rights online, establish clear transparency and accountability for online platforms and foster innovation, growth and competitiveness within the single market.

The DMA, instead, is concerned with economic imbalances, unfair business practices by gatekeepers and their negative consequences, such as a weakened platform market contestability. It identifies core platform services, characterised by highly concentrated multi-sided platforms acting as gateways for business users to reach their customers and vice-versa, and possibly displaying unfair behaviour vis-à-vis economically dependent business users and customers. It sets the conditions for core platform providers to be designated as gatekeepers, to be held to a number of stringent obligations and prohibitions. Market investigations, conducted by the European Commission, would lead to the designation of gatekeepers, the level of their compliance with the DMA provisions and new services and practices to be subjected to a more stringent regulation. Considerable investigative, enforcement and monitoring powers would be entrusted to the Commission.

To ensure digital market competition and fairness, the DMA and DSA highlight the need to introduce a regulatory balance that does not penalise the high rate of innovation that characterises this sector and ensures its success, both in economic terms and in the provision of services that improve user welfare and protection. The growing popularity and market power of the large platforms has,

however, spurred the European Commission to seek forms of regulation and ex-ante controls aimed at limiting dominance phenomena and increasing the accountability and transparency of digital services providers suited to the market's strong dynamism and flexibility.

In an attempt to understand the effects of these measures, it is important to stress that digital markets, in all their forms, are highly adaptable and innovative, with products and services that have not only radically transformed entire economic and business sectors, but also important spheres of human sociality, communication and entertainment, in just a few decades or, in some cases, even less.

The achievement of the mass deployment of such products is to a large extent attributable to the numerous new features resulting from the technological disruptions of the last decades, which make digital markets radically different from traditional ones. Firstly, the presence of the so-called "network effects" is of paramount importance and, through self-reinforcing dynamic elements, provides a combination of the traditional concepts of economies of scale and scope. To this, it should be added the use by digital intermediaries of market strategies aimed at enhancing user engagement, with the introduction of zero-pricing techniques and the use of algorithms and tracing. A third crucial element of digital markets is the accumulation and exploitation of immense amounts of data. This allows for the tracking of users in order to personalize services and content, and facilitates the expansion of one's sphere of influence into neighbouring markets through the bundling of a wide range of digital services. Moreover, the central role that these platforms have achieved regarding fundamental rights, content sharing and sensitive data management have increased their social responsibilities and require a greater participation and cooperation with authorities and expert users (e.g., trusted flaggers) in tackling illegal online activities.

While some of these characteristics have the potential for and, in many cases, have led to abuse and misbehaviour by digital players, it would be unfair to overlook the huge net benefits that they have given and continue to bring to end-users all over the world, as well as in the European Union. For business users, digital innovation means a key challenge and sometimes comes with heavy costs in terms of displacement, as is the case for any important technological changes. However, the availability of unprecedented opportunities brought by digital intermediaries and platforms in reaching new markets (i.e. digital advertising and exporting are perhaps the two most visible tools) is key to the current and future competitiveness of millions of companies, especially for SMEs that have had to face huge barriers to scaling-up in the traditional economy. Of course, large platforms are instrumental in maximising these benefits, matching businesses with consumers at a higher and more efficient level. Therefore, the policy objective should be, on the one hand, to ensure that fair conditions always apply to digital transactions and, on the other hand, that innovation is not stifled either by a stable monopolisation or over-regulation.

As for market dynamics, we have witnessed sudden and radical shifts in the composition of market shares, which highlight the high level of competitiveness digital platforms are exposed and confirm

a fair degree of scalability of many of these sectors. On the other hand, in some circumstances, we need to be beware of a too sizeable drop in competition ('tipping'), leading to a monopolisation or quasi-monopolisation.

The relationship between innovation and competition is indeed extremely complex, even more so in digital markets where new technologies and business models risk becoming obsolete and outdated within a few years. While competition among companies is essential for innovative developments and for the welfare of business users and consumers, so is the prospect of a return on the innovative efforts and investments of the companies themselves. Therefore, excessively restrictive regulatory regimes risk being harmful both in terms of technological development and competition on price, variety and efficiency.

1. The digital market segments in the convergence era

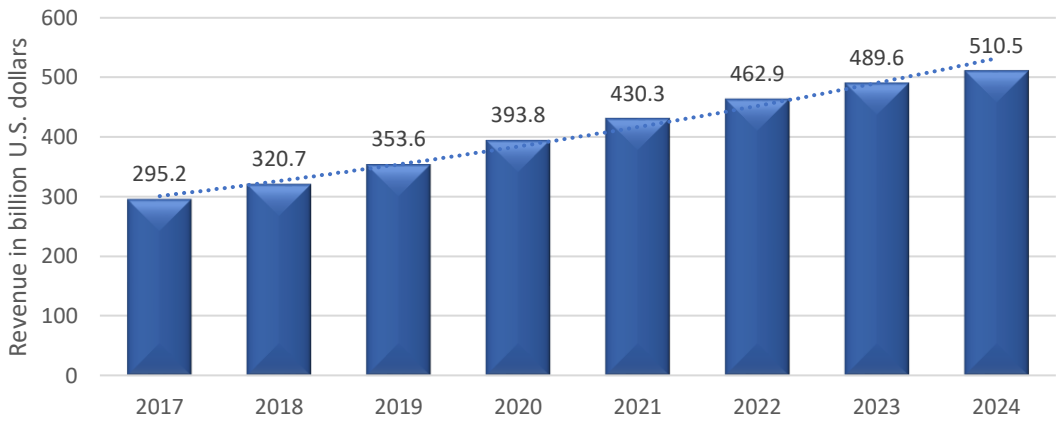
1.1 Market places and e-commerce

Recent years have seen a substantial increase in the activities and volume of online commerce in Europe both in terms of goods and profits. According to 2019 data, on average, e-commerce accounted for almost 20% of the turnover of European companies, with values exceeding 20% in ten EU countries (EU-28) and 30% in the Czech Republic and Ireland. The shift of many businesses to digital platforms has been strongly driven by the possibility of reaching a much higher number of users and consumers and, hence, higher profits. From 2017 to 2020, the total turnover of all European e-commerce increased by more than 25%, from $295 billion to $393.8 billion among the EU-28 countries. Strengthened by the acceleration caused by the global pandemic, the forecasts for the coming years continue to show very wide margins of growth for this sector. Total revenues are expected to reach $450 billion in the next two years and exceed $500 billion by 2024.

The Covid-19 pandemic, and the distancing requirements that have radically changed the shopping habits of millions of citizens across the continent, have opened the doors of online retailing to many users who had not previously used it. According to the Global Web Index (Q3, 2020), 76.8% of the sampled global population answered 'yes' when asked if they had made any type of purchase online, on any platform, in the past month. This percentage is impressive, especially considering the reduced possibilities of developing countries in terms of access to the Internet and digital devices. Amongst European citizens using the Internet the most during the period selected by the survey were the British (85.5%), the Germans (81.6%) followed by the Austrians (81.3%) and, in fourth place, the Italians (79.7%). It is also worth noting the high number of Asian countries amongst those that make most use of online marketplaces.

Although the use of e-commerce is now widespread, it still has a limited impact on national economies in terms of its contribution to GDP. According to data from the Statista Digital Market Outlook 2021 and The World Bank, China is the only country in the world where online consumer spending as a proportion of national income exceeds 10%. This figure is much lower for European countries (the UK at 4%, Poland at 3.7%, Germany at 3% are at the forefront, while in Italy the ratio is 1.9%). Also the United States is low at 2.6% of total income.

Figure 1: European[2] retail e-commerce revenue forecast (in U.S. $, bln)



Fonte: Statista 2020

By focussing on the main active platforms in the sector, it would appear that Amazon is the main digital marketplace in Europe, with 1.1 billion visits per month, which represent about 20% of the total users of the US web giant. Considering that Europe and the US are more or less comparable in terms of GDP and population, it is interesting to highlight that, in the United States alone, Amazon has a market volume that is double that in Europe (around 2.3 billion visits per month). This is an indication of the increased online competition that Amazon is forced to face in the European market, where, in addition to the presence of the other American major player eBay, recent years have also seen the expansion of numerous EU-based marketplaces. Examples of these are Zalando, a German fashion company that is challenging Amazon for the e-commerce supremacy in many northern European countries, and also the British Asos and the French PriceMinister. The latter represent the high degree of flexibility resulting in the share of the e-commerce market varying according to the different geographical macro-areas.

A clear dominance by Amazon and eBay, in fact, seems to be fairly confined to the United States, where the two platforms together account for almost 80% of the entire market. Even in Latin America, the two companies have reached much smaller market shares, with the MercadoLibre[3] platform largely leading in Brazil, Mexico, Argentina, Colombia and Chile, and together account for around 86% of online sales in Latin America. Moving on to the Asian markets and, in particular, China, the US giants are almost entirely eclipsed (Amazon China has a market share of less than 1%) by the dominance of local players such as Alibaba/Aliexpress, JD and Suning.

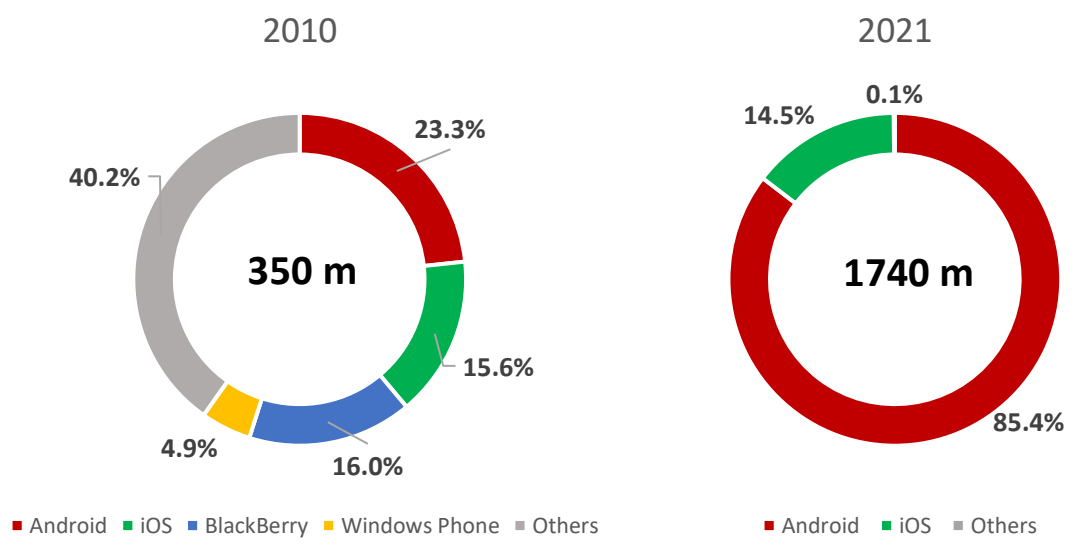
[2] It includes the following countries: Albania, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom.

[3] https://seekingalpha.com/article/4372121-mercadolibre-tale-of-two-markets

1.2 Operating systems and app-stores

The latest figures released by GSMA Intelligence show that two-thirds of the world's population now use a mobile phone. This figure has been almost constant over the past few years and corresponds to about 85% of all people aged 13 and over in the world. In just a decade, the smartphone has become an indispensable tool in the daily lives of millions of people.
While the market for companies producing smartphone hardware is still competitive, the entire market for the software that enables these devices to operate has consolidated around two companies, forming a global duopoly in which the two incumbents, Google Android and iOS, together account for 99% of the market. We are therefore witnessing a very different scenario from that of 2010, when Windows Phone and Blackberry were also active, and when Android and iOS together 'only' made up 38.9% of the market.

Figure 2: The global market for mobile operating systems: a stable duopoly equilibrium?



Source: Own elaboration from IDC data

Analysing the use of the two operating systems for each country, it is interesting to note that Google Android is the most widely used system in most parts of the world, as it is available for a large number of manufacturers. However, as evidence of the complexity of technological competition, it should be also highlighted that in Japan and the United States, two of the most advanced markets in the world, Apple is the leader with over 50% of users. This wider spread of Google's owned software also stems from its open-source nature, which allows it to be used on a wider range of hardware and leaves room for the development of new operating systems (even if other versions based on Android source code never really took up). However, the real effect of pre-installing software and apps on a device is still unclear in terms of effective usage. If, on the one hand, the

distribution of Google Play Service (GPS) apps and of its most popular services (Google Search, Gmail, Google Maps, Chrome, Google Play Store, YouTube) is under investigation[4], on the other hand, the number of downloads and the usage of these apps also in rival OS devices (e.g., YouTube, Google Maps, Chrome) show that some services simply spread because of their excellent functioning.

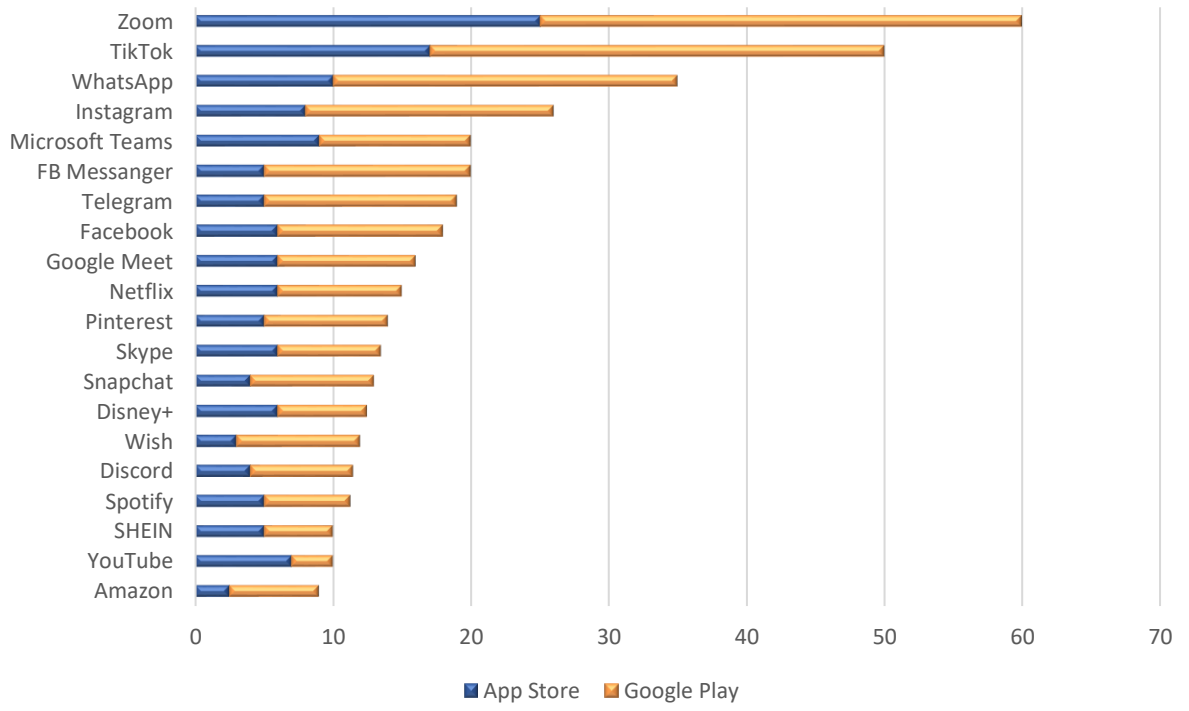
As further proof of the complexity of these markets, the HarmonyOS project launched in 2019 by Huawei should be mentioned, as it could undermine the market equilibrium being consolidated over recent years. Since 2012, the Chinese leader has been working on the switch from Android to its own platform, however, the recent ban imposed by the US has now made this transition both urgent and necessary, speeding up the schedule for its deployment. The HarmonyOS 2.0 Developer Beta system for smartphone app developers was launched in December 2020 (with endorsements from numerous Asian players such as JD.com, Baidu, Youku), while between April and October 2021, HarmonyOS will be opened to most devices. Indeed, in addition to its own products, Huawei's operating system will be available to all manufacturers that join the "hardware ecosystem", and so far involving companies such as Midea, Joyoung, and Robam. Considering the speed of innovation in these sectors, together with the large customer base in Asian countries and the quality generally achieved by Chinese hi-tech, this could lead to a further global reassessment in the operating system market quotas over the next decade.

Closely linked to the analysis of operating systems is the market segment covering app stores and apps themselves. Indeed, apps have become the central function of smartphones, and are the services where mobile users now spend most of their time. Based on January 2021 estimates on Google Android users, time spent on mobile devices has now exceeded an average of 4 hours per day - 44% being spent on content sharing, communication, and social media, while 26% is spent on entertainment and video apps, and 9% on video game apps.

Therefore, it is not surprising that among the apps with the largest number of users we find all the major social media apps, followed by e-commerce apps, such as Amazon, and entertainment apps such as Netflix and Spotify. The popularity of social networking apps is also reflected in the number of downloads, an important indicator of the popularity of these services. Facebook is the most downloaded app, followed by Messenger, WhatsApp, Instagram, Snapchat and Skype. However, when analysing the number of downloads for the different stores (App Store for iOS and Google Play for Android), it should be taken into account that many apps have recently become part of operating system deals, meaning that they are pre-installed in the mobile device and, therefore, do not need to be downloaded. This creates some issues concerning the significance of the download statistics, as these might not entirely correspond to actual app usage. As reported in the previous paragraphs, this is the case with many of Google's own apps, but it has also recently become the case for the most popular social media apps, entertainment platform apps and e-commerce apps.

[4] https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws

Figure 3: Overall App Downloads in Europe[5] (Q2, 2020) (in millions)



Source: Statista estimates

Globally, 2020 has shown important growth rates, both in terms of absolute downloads (+7% on 2019) and app spending (+20% on 2019). During the year, the most downloaded app worldwide was, for the first time in history, China's TikTok, which, despite Trump's geopolitical obstruction, managed to snatch the lead from WhatsApp, which topped the ranking in 2019. TikTok's app is followed by the main social networks - Facebook, WhatsApp, Messenger, and Instagram (all owned by Facebook)-, while great dynamism in the sector has also been highlighted by the (presumably inevitable) surge of platforms specialising in video calls and online video-conferencing. As a result of the pandemic, these have experienced an unprecedented growth over the last year, with Zoom becoming the most installed app in 2020 in Europe with almost 300 million downloads worldwide, 60 million being in Europe alone, while Google Meet and Microsoft Teams stopped at 110 million and 70 million respectively (16 and 20 million in Europe). Skype, historically considered to be the forerunner of the video-call sector, has dropped out of the ranking.

[5] It includes the following countries: Albania, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro, the Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom.

This data clearly demonstrates that the digital sector is still a very competitive and contestable realm, with new entrants able to succeed in a very short timeframe, thanks to the same factors (i.e. network effects) that have often been pinpointed as being proof of resulting in the exact opposite.

1.3 Social networks, sharing and video

When referring to social network platforms, we consider the wide range of services that allow end users to connect, share and communicate with each other through text, video and images. Due to recent convergence, this market sector now includes both the traditional social networking services, created to foster the creation of communities through the sharing of digital content, and the platforms that, by connecting to the Internet, allow text and vocal messages to be exchanged in real time. In addition, there are platforms allowing for creating, streaming and sharing video and photo content, which are in many ways a novelty for the sector.

Although each of these categories of services would deserve an in-depth individual analysis, it is extremely complex to identify clear boundaries and distinctions between them. In fact, there are now numerous cross-sector platforms, which are continuously seeking to expand their range of possibilities and services aimed at increasing user-friendliness and opportunities, as well as customising their services according to new trends or consumer preferences.

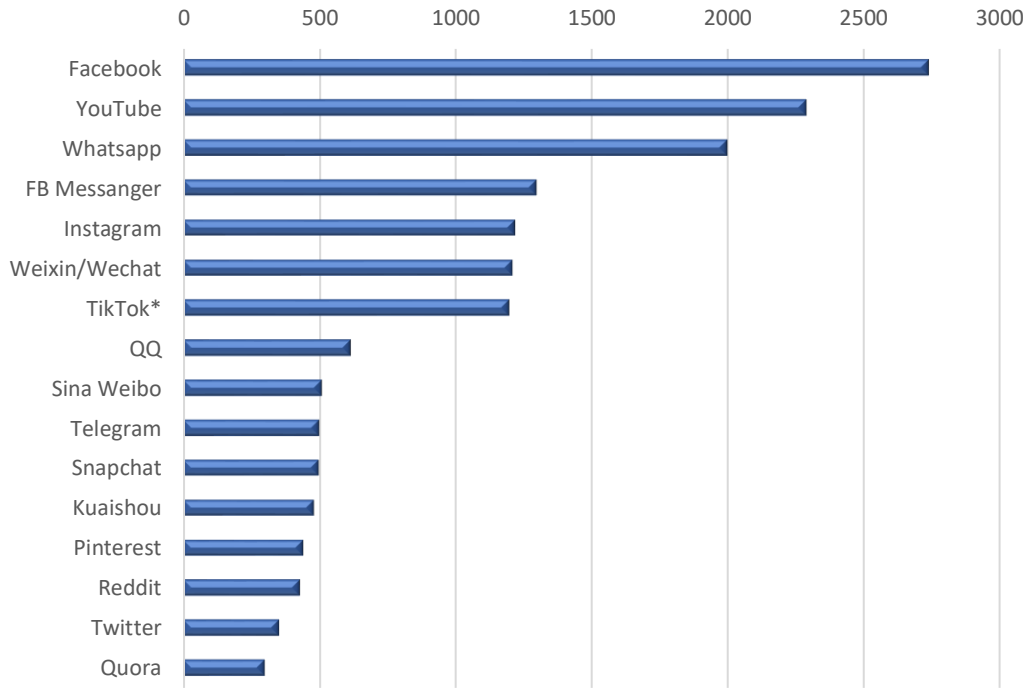
One of the most common examples of this is WhatsApp Messenger, which was launched in 2009 as a service for instant communication via text messages, and has since developed possibilities for sharing messages in voice format, documents, photos and videos, and even geo-localised locations. Similarly, continuous evolutions have also made it rather complicated to find clear distinctions between video-sharing services like YouTube and social networks like TikTok, both in terms of audience and market boundaries.

The economic value of these platforms, and their dominance in the market, is mainly dependent on the number of users they attract and on the subsequent turnover linked to advertising services that rely on the huge amounts of data they collect. The population coverage of these services is, therefore, crucial and has resulted in a clear global growth over the last years. By the end of 2021, the total number of social media users will be close to 4.9 billion, with a growth rate of 13% over the last year. An equally significant increase is revealed in Europe where, from 2011 to 2019, the number of people using social networks at least once a day more than doubled, reaching 48% of citizens.

On a global level, according to Kepios 2021 data, the social media platform with the highest number of users is Facebook, with about 2,740 million users and growth rates that every year approximate 10% (in 2020 a +12% was recorded, the highest figure in the last four years). With boundaries becoming ever more flexible and indistinguishable, the main services that monitor the spread of

social networks bring together traditional social networks, video-sharing apps, interpersonal communication services and hybrid players. In second place, we find YouTube, the world's leading video-sharing site and the second most used website in the world (behind Google itself). This is followed by WhatsApp and Instagram, both owned by Facebook, and Weixin/WeChat, the Asian giant that dominates the eastern market, thanks in part to the ban on numerous US apps in China.

Figure 4: World's most-used social media platforms (active users, mln)



Source: Kepios Analysis (2021)
*** the figure considers both the users of TikTok and of the Chinese market version, Douyin**

Also exceeding 1,200 million[6] total users is the Chinese social network TikTok, which, after being launched in 2016, has rapidly scaled the market thanks to its innovative video sharing services offered in more user-friendly and viral formats. In just four years, the app has now been downloaded more than 2 billion times in the Google Store and iOS App Store, becoming, in 2019, the most downloaded app in the latter. During 2020, TikTok was the second most downloaded app both globally (300 million) and in the European market (50 million), with an average of 1 million video views per day. To appreciate the spread of this platform in relation to the growth of other social networks, one only needs to recall that Instagram took six years from its launch to gain the same amount of monthly active users that TikTok managed to achieve in less than three years, while

[6] Calculated as TikTok+Douyin

Facebook took more than four[7]. This shows the great permeability of a market that is increasingly open to innovative solutions, content and user-friendly methods.

In addition to the growing popularity of video and music content, perhaps the most interesting trend in the evolution of the social sector is the use of these platforms as search engines. According to GWI 2020 data, around 45% of global Internet users now claim to turn to social networks at least once a month when searching for information on products or services they are considering for purchase. This value is considerably higher among younger age groups (16 to 24 years old), who are now more likely to start their product and brand searches directly on social networks rather than turning to a traditional search engine, according to the researchers.

1.4 Search and Ads

General search services allow consumers to find answers and information in a matter of seconds on anything by entering any keyword in a search engine platform, which then uses algorithms to evaluate the relevance of information on all publicly available webpages. The search engine delivers results within few seconds and it also includes ads in various forms. At first, the search engine market was exclusively accessed through computers but, recently, mobile devices have represented the largest and fastest growing search distribution channel. Being funded by ads, search activities are based on the collection of the users' personal information and preferences. Scale is therefore a crucial element in these markets, since, as the number of search engine users grows, advertisers benefit from a greater dissemination and visibility amongst a larger audience of potential buyers. Scale also allows for improved and more efficient automated AI learning algorithms, which make use of massive databases to deliver results which are even more relevant and personalised.

Massive user-bases and scale, together with very large costs and initial investments, have led to a global market structure which is extremely restricted and concentrated. Currently, there is only one leading provider - Google - and another four important players - Bing (2.7%), Yahoo! (1.5%), Yandex (1.5%) and Baidu (1.4%). However, it is worth noting that, also in this market, technological trends are challenging the dominant players as well, as they seem to be constantly looking for new updates or formats in order to maintain their position.

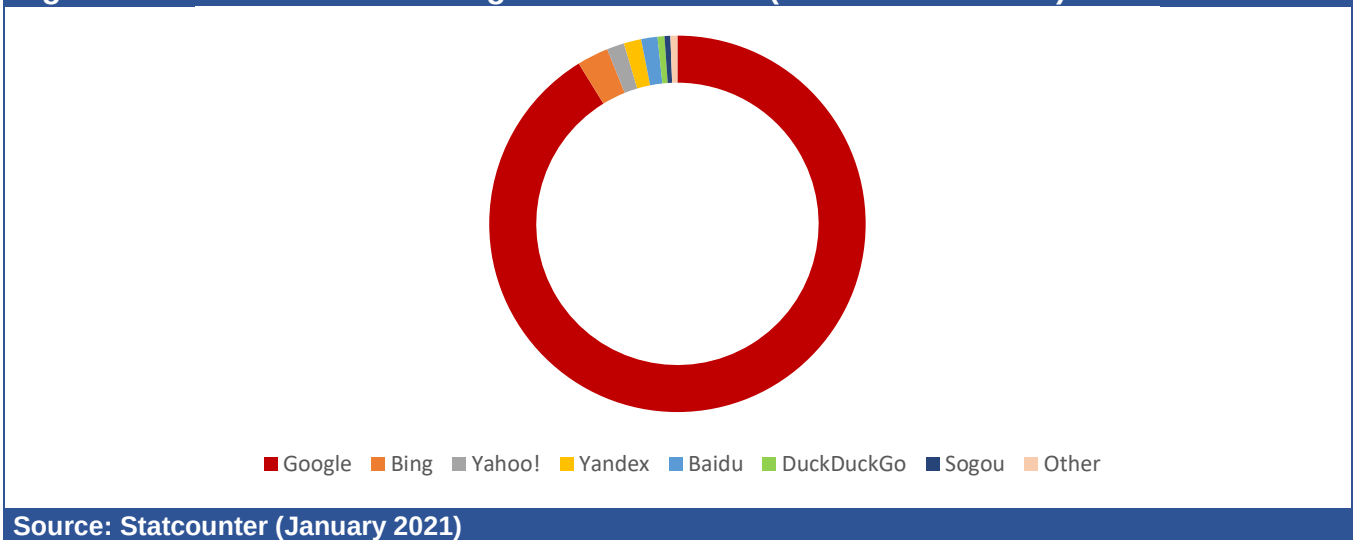
Today, Google is by far the most commonly used search engine in Europe, covering more than 85% of desktop search queries in the five largest European countries (Italy 91.7%; Spain 91.2%; Germany 85.6%; France 85.2%; the UK 85%). This trend is also confirmed in India, Australia, Japan and, predictably, in the U.S., where its market position has even grown in the recent years, following an increasing trend beginning in 2014, and now making up almost 90% of all search engine queries.

[7] Source: Oberlo on DataReportal 2021

Microsoft Bing and Yahoo (based on the same Microsoft technology) are the second and third most commonly used search platforms in Europe, but have a much smaller market share compared to Google. The other providers are based on mainly national users, with Yandex (60% of local market share) and Baidu respectively dominating the Russian and Chinese markets. Notwithstanding the strict geo-political restrictions on US search engines that determine the Chinese market composition, it is interesting to see that Google ranks second[8] in China behind the market leader Baidu, highlighting the quality of attractiveness for users all over the world. The above aspects shed a light on the many difficulties that arise when evaluating Google's dominant position, as this is clearly not only determined by lock-in and scale effects, but is also attributable to the undisputed quality that is provided by the service. Moreover, Google search engine has resisted the competition coming from Microsoft (first with Live Search, then with Bing and Yahoo!, which uses the Bing algorithm) which could rely on pre-installation in the Windows operating system. A similar trend has taken place in the browser market with the challenge of Internet Explorer, Firefox and Google Chrome.

An element of dynamism and a potential increase in competition in this market can be seen in the very high increase in the usage rates of smaller search engines during 2020. In fact, although still being very small in absolute values, both DuckDuckGo (+40%) and Sogou (+60%) have shown an impressive growth that, together with the growth rates of the larger Yandex (+38%), Baidu (+28%) and Bing (+6%), if persistent over the next few years, could begin to undermine Google's dominant position.

Figure 5: Global web search engine market share (% of search traffic)

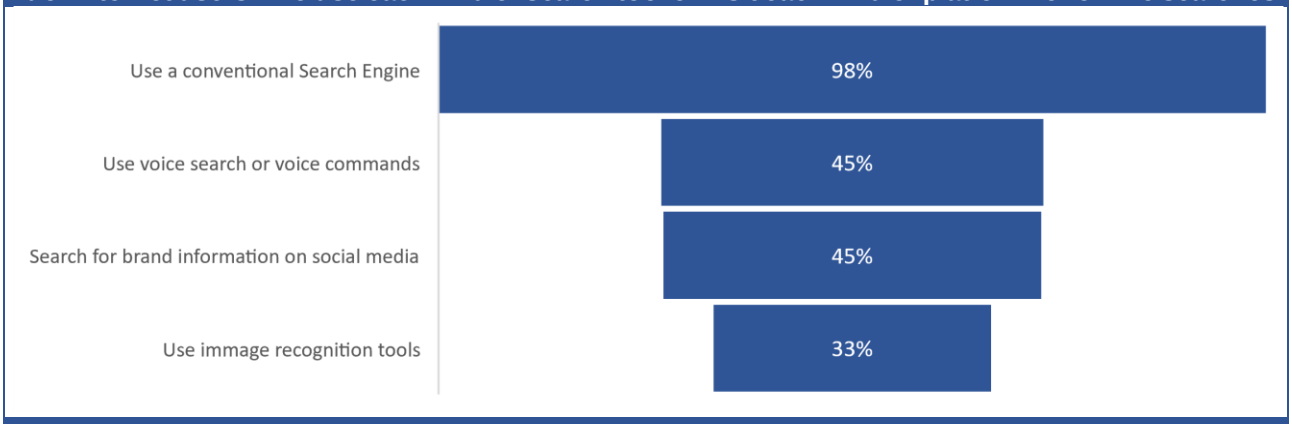


Source: Statcounter (January 2021)

[8] Statista 2019 Global Consumer Survey

However, as already mentioned, a perhaps even more significant element that could shake up this market segment is the growing importance of "non-conventional" search methods. These include the use of voice search technologies or voice commands, the use of social media platforms for commercial information search, and the use of image recognition tools on mobile devices. These new technologies and user-friendly approaches are regarded as the new frontiers of the search market, and may even eventually undermine today's well-established market dynamics.

Figure 6: Online global search behaviour
% of Internet users who use each kind of search tool or visit each kind of platform for online searches



Source: GWI, Q3 2020

The increase in the usage of social media platforms as services to access commercial information searches is also reflected in the advertising market data, which follows the general shift from desktop to mobile devices. From 2019, mobiles have become the main device type for global digital advertising spending (52% mobile, 48% desktop) and are now expected to take on an unchallenged dominance in the upcoming years (reaching 65% in 2025).

From a global perspective, digital advertising revenues are expected to grow from the $355.6 billion of 2020 to $491.1 billion by 2025 (+6.7%). Compared to the U.S. and the Chinese markets, Europe shows the strongest forecasted growth for the period (+6.9%), although still being forecasted as the smallest market out of the three in terms of market volume for 2025. Analysing the various advertising channels, social media ads present a +7.2% predicted growth in the same period, with Europe again showing the highest average forecasted rate (+7.4%). Another factor affecting a higher revenue per user may also be seen in the near future due to a shift towards more complex formats, such as video content.

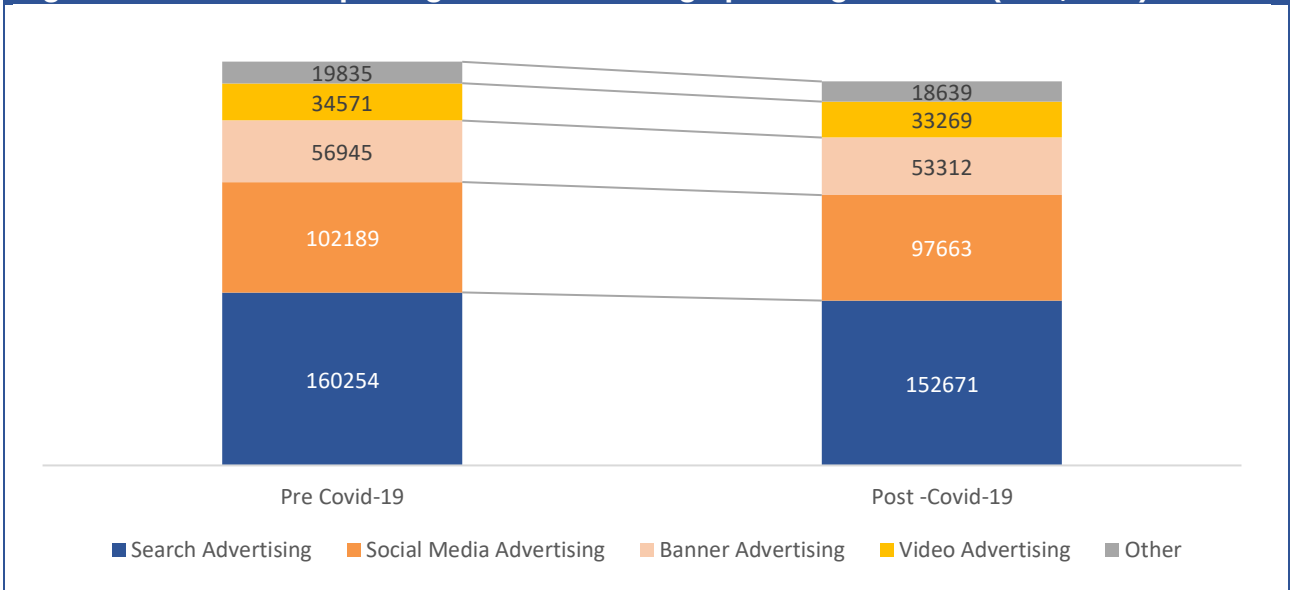
It is worth noting here how digitalisation is also making it very complicated to analyse the advertising market, as different "channels" and formats are now not only converging, but also creating different subsectors in which players from different environments compete for consumer attention.

The segmentation presented in Figure 7 differentiates between search (the biggest segment), social media, banner (appearing in websites other than social and search engine), video and classified. However, as noted above, converging technologies and strong competition for consumer attention has increasingly blurred the boundaries, so that, for instance, both social media (such as Facebook and TikTok) and video sharing platforms (such as YouTube), as well as potentially personal communication tools such as WhatsApp, compete for video consumption on different formats and devices, making it extremely challenging to define the relevant markets.

In general, according to Statista's data, at global level, the pandemic had a strong impact on the advertising industry in 2020, as ad spending is historically strongly affected by GDP changes and consumption trends. As a whole, the industry suffered a -4.9% contraction in profits, with traditional channels, such as banner ads (-6%) and search ads (-5%), being the most affected. On the contrary, as a consequence of the digital acceleration over the last year, social media and video have been the least affected, even though these have also seen significant decreases in business (both -4%) regardless of the important increase in social media usage and engagement during the pandemic.

The leading platforms, classified as the share of advertising spending, all hold a global market share that hovers around 10%. The most successful platform is once again Google (10.5%), closely followed by the Walt Disney Inc. (10.4%), NBC Universal (9.2%) and CDS Corp. (8.6%). Numerous other platforms hold smaller shares, but still represent important active players in the market. These include Facebook (4.8%), FOX Corp. (4.2%) and Discovery (3.8%), while Microsoft has a much smaller share (1.9%).

Figure 7: Covid-19 impact: global advertising spending forecast (mln, US$)



Source: Statista Digital Market Outlook, 2020

1.5 Cloud

Cloud computing has been defined by NIST (the US National Institute of Standards and Technology) as "an elastic execution environment that provides network and on-demand access to a shared set of configurable computing resources (network, servers, storage devices, applications and services) in the form of services at various levels of granularity. These services can be rapidly requested, provisioned and released with minimal management effort on the part of the user and minimal interaction with the provider". In general, cloud computing involves two components. The first is the cloud infrastructure, which consists of the hardware resources required to support the cloud services being provided and typically includes server, storage and network components. The second component refers to software applications and computing power for running proper or third-party business applications.

Cloud computing services allow individuals, businesses and organisations to flexibly use both their own ICT resources, or, instead of building or expanding their own IT infrastructure, to access computing resources hosted by third parties, namely specialised 'cloud providers', on the Internet. It is worth noting here that the purpose of the cloud is not to disseminate information on a large scale, but to offer a secure space where users can store their personal data. The data stored in the cloud is used only by the owners and by a limited number of users authorised by the former. Indeed, the ownership of the data uploaded to the cloud remains with the user and is not transferred to the provider, profiling these services as being quite different from social networks and other platforms for content sharing. For this reason, imposing a control on user data does not seem to be an appropriate measure considering its technical characteristics and business model, and would risk jeopardising user privacy, resulting in the cloud losing one of its main competitive advantages.

In market terms, the world industry of new digital technologies is expected to reach €2.2 trillion by 2025, revealing that Europe has a strong interest in participating in the technological race by strengthening its position and by cooperating with other major international players. This is particularly relevant for the data market, which is at the core of cloud activities. According to the data released by the IDC European Data Market Monitoring Tool (2020), which measures the impact of European data market activities on the economy as a whole, the total value of the data economy exceeds €350 billion for the EU Member States (2020), up 9.2% compared to 2019. The market growth rate is expected to expand further in the coming years, with the EU baseline scenario predicting a total value of €550 billion for the EU countries in 2025.

Analysing the market share of the different cloud providing platforms, the top 8 vendors account for over 70% of global trade (making up the so-called “hyperscalers”, with the global scale, expertise,

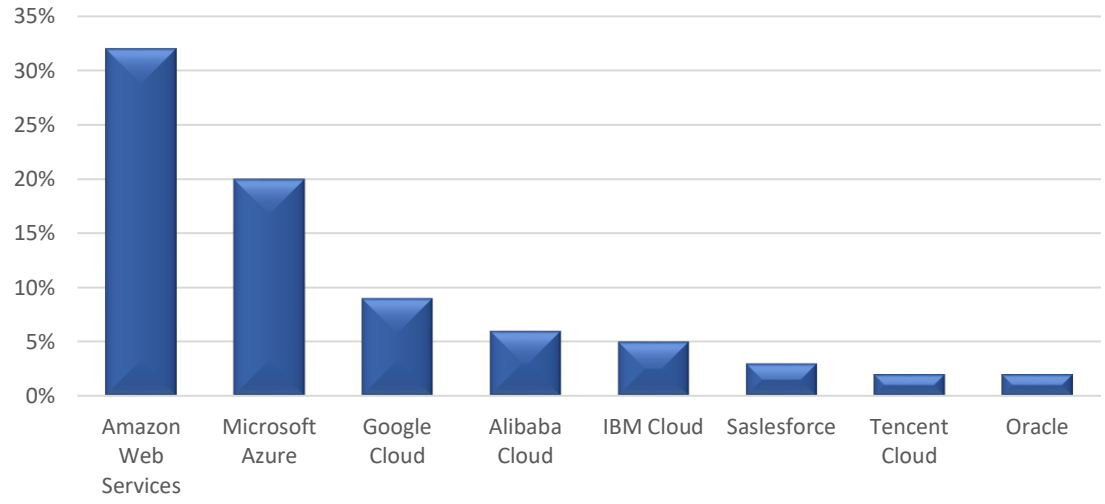
cutting-edge innovation and broad range of services needed to maximise cloud value[9]). The $130bn worth market is led by Amazon Web Services (AWS), which holds roughly a third of the global market share, followed by Microsoft Azure with approximately 20%, and Google Cloud, Alibaba Cloud and IBM Cloud all below 10%. Over the last five years, Amazon has retained its market share, while, instead, Microsoft Azure and Google Cloud have doubled their quotas. The former climbing from 9% in 2015 to 20% in 2020, and the latter from 4% to 9%. This shows a clear space for growth and expansion, at least for the largest tech players.

The global cloud computing market size is expected to grow from $371.4 billion in 2020 to $832.1 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 17.5% during the forecasted period. Seeking to protect their strategic information and, at the same time, make the most of the economic opportunities arising from the data economy, several EU Member States have started to develop independent digital autonomy strategies, with the aim of countering or at least regulating the current trend, where European companies and public administrations use cloud services provided by non-European operators, especially from the US or China. However, these attempts to create national cloud infrastructures have not always achieved their objectives, opening the path for the EU Commission's "Gaia-X" Cloud Project. This federated and transversal data infrastructure would allow the Union to guarantee determined standards of privacy and security and, at the same time, to better exploit the economic opportunities deriving from the data market.

The importance of the cloud is becoming increasingly acknowledged among European companies and other players. Compared with 2018, the use of cloud computing has increased by 12 percentage points, with 36% of EU enterprises reporting to have used cloud computing in 2020. According to 2020 data, released by Eurostat, significant differences can be observed across countries in terms of cloud usage. Northern countries report the highest firm adoption rates, with Finland (75%), Sweden (70%) and Denmark (67%) leading, followed by Italy and Estonia where more than 55% of enterprises used cloud computing. On the other hand, in Greece (17%), Romania (16%) and Bulgaria (11%) less than 20% of enterprises did so.

[9] Accenture (2020), *Hyperscale your cloud journey: Partner for more value*.

Figure 8: Market for cloud infrastructure service providers (Global market shares*)



Source: Synergy Research Group, Q4 2020
*** Includes PaaS and IaaS, as well as hosted private cloud services**

2. The online dissemination of illegal and harmful content and institution and main platform initiatives

Digitalisation is revolutionizing business models and the relationship between authorities and citizens, and between enterprises and consumers, creating new opportunities, but also raising some critical issues.

According to the EU institutions, European citizens are exposed to increasing risks and harm online, due to the spread of illegal activities, infringements of fundamental rights and other societal damage. These issues, which are widespread across the online ecosystem, seem in some way to be concentrated in the very large online platforms, due to their wide reach and larger audiences.

Online illegal activities include, amongst others, practices such as the dissemination of illegal content (fake news, hate speech, terrorist content, child abuse material and illegal ads), illegal marketing services (or infringing consumer protection provisions) and the sale of illegal goods (dangerous or unsafe goods, counterfeit goods, scams, illegal medicines and so on).

According to the results of the survey conducted by Eurobarometer for the EU Commission out of over 30,000 Internet users in all Member States, about 60% of respondents believe they had seen at least once some sort of illegal content online. Scams, frauds or other illegal commercial practices had been experienced by 41% of the interviewed people, while 30% had seen hate speech, 27% counterfeited products and 26% pirated content.

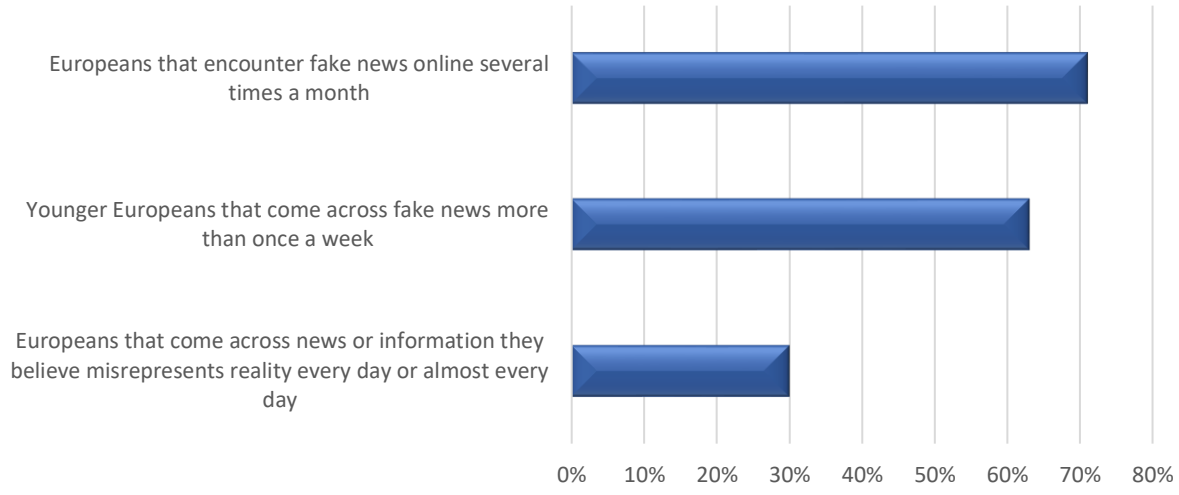
In this scenario, large platforms play, today, a key role in distributing and shaping information online, assuming a responsibility that, although not definable in typical editorial terms, seems to go far beyond the mere technological aspects. For these reasons, their design choices and security practices have a strong influence on user safety online, having the power to shape online contents and discussions as well as digital trade. In the current situation, to stem the spread of such harmful content and protect their users, organisations carry out careful moderation and monitoring of published content.

2.1 Online disinformation

Online disinformation, including misleading or outright false information, is a major challenge for Europe and poses a considerable threat to the future of democracy. The spread of fake news risks eroding the trust in institutions and in the media, and damaging democracies by hampering citizens in being able to take informed decisions. According to the latest data of Eurobarometer (Fig.9), 71% of Europeans encounter fake news online several times a month (30% every day). Those who seem

to be most exposed are young people, which in 63% of the cases say that they encounter fake news at least once a week.

Figure 9: Eurobarometer disinformation data (2018)



Source: Eurobarometer

In order to face this potential threat, the European Commission published a Communication on Tackling Online Disinformation in April 2018, followed by the "Code of Practice on Disinformation", the first worldwide self-regulatory set of standards to fight disinformation. This was voluntarily signed by digital platforms, leading social networks and the advertising industry in October 2018, and signatories include Facebook, Google, Twitter, Mozilla, as well as from the advertising industry associations. In 2019, the Code was also signed by Microsoft, whilst TikTok joined in 2020, bringing the number of included platforms to 16. The Code focuses on several issues related to false online content, such as the use of misleading advertisements, fake accounts and online bots, and the need for transparency in political advertising. Each association or firm adhering to the Code presented an individual timeline containing the strategies for its implementation, and these were then monitored by the European Commission.

Starting from September 2020, the Commission started publishing the reports provided by the signatories of the Code of Practice as part of the COVID-19 monitoring and reporting programme set out in the Communication "Tackling COVID-19 disinformation - Getting the facts right". These baseline reports highlight how these platforms have intensified their efforts in fighting disinformation both in terms of promoting authoritative sources of information and in developing new tools and services to facilitate access to reliable content. Furthermore, direct actions against false content have also been implemented, with platforms demoting and removing content violating their updated terms of services and advertisements that exploit the crisis.

In terms of tackling fake news on COVID-19, data shows that all main players have directed their users to resources from the World Health Organisation (WHO) and other health authorities, and many have also created specific information pages or panels on the topic. Facebook and Instagram reported that more than 2 billion users visited their COVID-19 "Information Center", with 30 million EU users alone between July and August of 2020. From January to August 2020, Google blocked or removed over 82.5 million COVID-19 related ads and suspended more than 1,300 accounts from EU-based advertisers, while Facebook displayed misinformation warning screens associated with COVID-19 related fact-checks on over 4.1 million pieces of content in the EU in July and 4.6 million in August. In the same two months, TikTok applied a COVID-19 sticker to more than 86,000 videos across its four major EU markets (Germany, France, Italy and Spain) and tagged, globally, 7 million videos with words, hashtags or music related to COVID-19 information. Furthermore, Twitter reported that 80% of the violating content on its platform was detected by its automated systems and that 2.5 million accounts were challenged under Twitter's COVID-19 guidance.

An update of the initiatives applied from January 2021 highlighted other important results achieved. For example, Twitter launched on 26 January a new Academic Research Tool in its API to give researchers free access to the full history of public conversation and to additional features. Fact checks published by fact-checking organisations from EU Member States have appeared in Google Search about 6 million times a week on average, which adds up to more than 30 million impressions generated since January 2020. In January 2021, on Bing, the panel "COVID experience" appeared when typing COVID-related searches, and had more than 18 million visitors globally, including 2.9 million from EU countries. Facebook, in January 2021, removed over 13,000 pieces of content related to COVID-19 in the EU for containing misinformation that could lead to imminent physical harm, and over 9,000 pieces violating its medical supply sales standards. As for TikTok's COVID Centre Page, across Italy, Spain, France and Germany, the total page views amounted to 78 million and user views to 23 million.

Last May, the Commission presented a Guidance to strengthen the Code of Practice on disinformation, aiming to evolve the existing Code of Practice towards a co-regulatory instrument foreseen under the Digital Services Act (DSA). The signatories should present a first draft in Autumn 2021 to strengthen the Code, based on three datasets and best practices: the assessment of the first year of the Code, the experiences of the 2019 European Elections and the COVID-19 Disinformation Monitoring Programme.

The reinforcement of the Code of Practice should support an adequate visibility of reliable information of public interest and reduce the monetisation of disinformation. Other key aspects concern the step-up of fact-checking and the strengthening of cooperation between signatories and fact-checkers, as well as ensuring effective data disclosure for research on disinformation. To conclude, it seems important to put in place a robust monitoring mechanism to ensure transparency and public scrutiny of the effectiveness of the signatories' actions.

2.2 Hate speech, terrorist content and protection of minors.

According to the United Nations definition, the term **hate speech** is understood as any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are. In other words, it is based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor.

Many countries approved laws that restrict hate speech, including European Member States such as Denmark, France and Germany, as well as the United Kingdom. The main difficulties lie in finding the right balance between protecting people and guaranteeing them freedom of speech. It is worth noting here how the transnational nature of the Internet makes it difficult to set universal limits or boundaries. According to the International Covenant on Civil and Political Rights (ICCPR), "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility, or violence shall be prohibited by law".

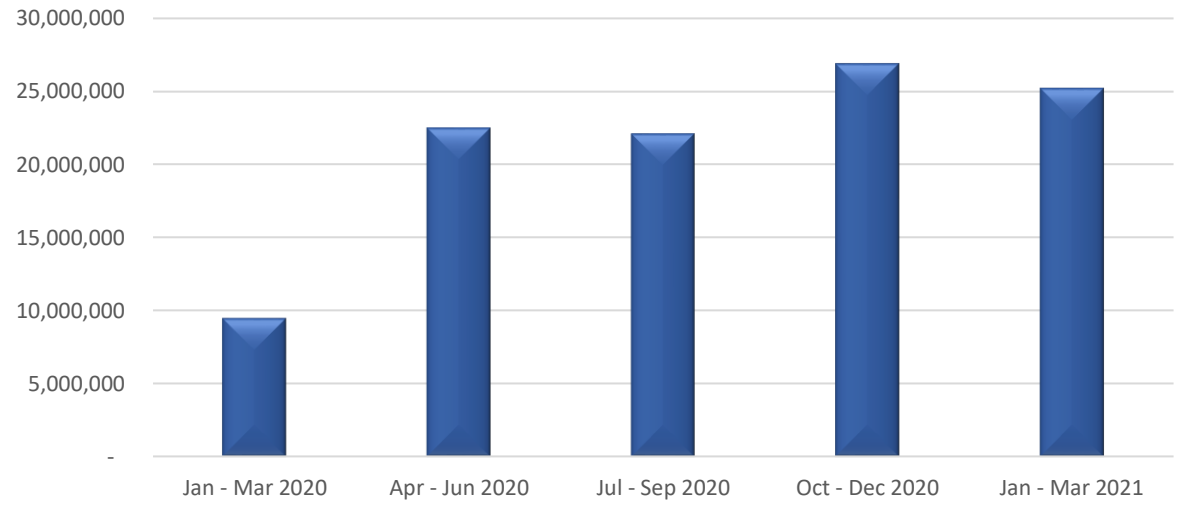
In 2016, several tech operators[10] jointly agreed on a European Union Code, voluntarily assuming the responsibility to review the “majority of valid notifications for removal of illegal hate speech" uploaded on their services within 24 hours.

In June 2020, the European Commission released the results of its fifth evaluation of the Code, finding that, on average, 90% of flagged content was assessed by the platforms within 24 hours, while 71% of the content deemed to be illegal hate speech was removed in 2020 (only 28% in 2016). Currently, according to the review, platforms continue to respect freedom of expression and avoid removing content that may not qualify as illegal hate speech. Moreover, operators gave feedback to 67.1 % of the notifications received.

Looking at the numbers, thousands of hateful content uploads appear on various web platforms every day. Data disseminated by Facebook on blocked malicious content (Fig.10) shows that, in the last quarter only, the social network acted against over 25 million content pieces of this kind. Unfortunately, the trend is increasing, and between the first quarter of last year and the same period of this year the hate content removed almost tripled (+165%).

[10] Namely Facebook, Google, Microsoft, and Twitter agreed to join the Code on 31 May 2016.

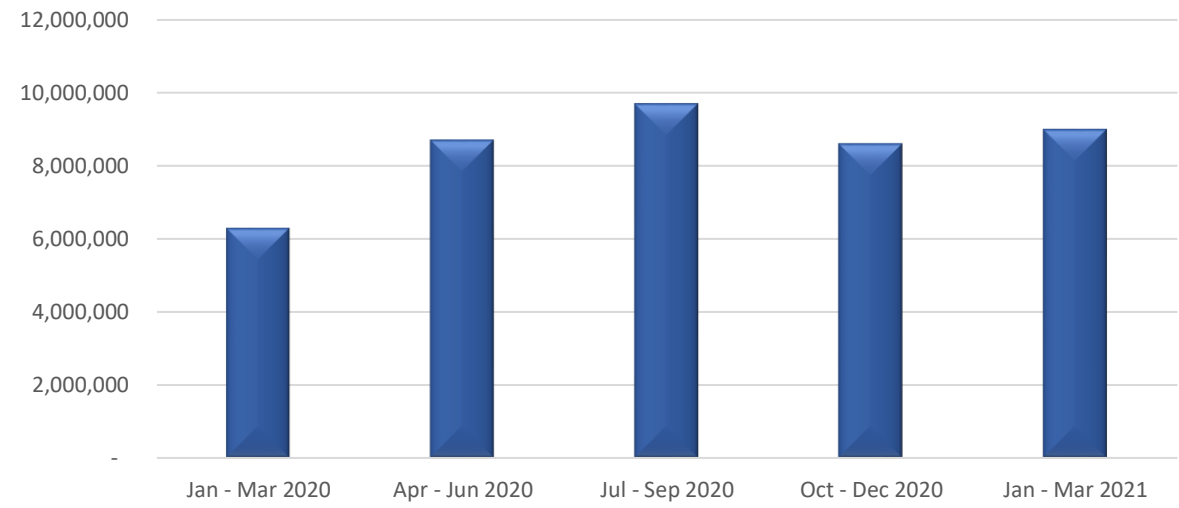
Figure 10: Hate speech content removed by Facebook



Source: Facebook

The social network must also deal with a huge amount of content flagged as **terrorist**. According to the latest data published, in the first quarter of 2021, Facebook blocked approximately 9 million terrorist messages (Fig.11). Unfortunately, also this figure is increasing if compared to the same period of 2020, though at a slower pace (+ 43%).

Figure 11: Terrorist content removed by Facebook



Source: Facebook

Similar issues were faced by Twitter which, in the first half of 2020, acted against 635,000 accounts and almost 1 million content pieces flagged as hateful conduct (Tab.1). To understand the magnitude of the problem, these accounted for about 50% of the total content removed for violating the platform rules.

Table 1: Accounts suspended and content removed by Twitter (Jan-Jun 2020)

POLICY CATEGORY	Accounts suspended	Content removed
Hateful conduct	635.415	955.212
Child sexual exploitation	438.809	10.343
Impersonation	120.066	12.484
Abuse/harassment	72.139	609.253
Illegal or certain regulated goods or services	54.070	16.663
COVID-19 misleading information	1.751	4.647
Civic integrity	-	2.710
Total	**925.744**	**1.927.063**

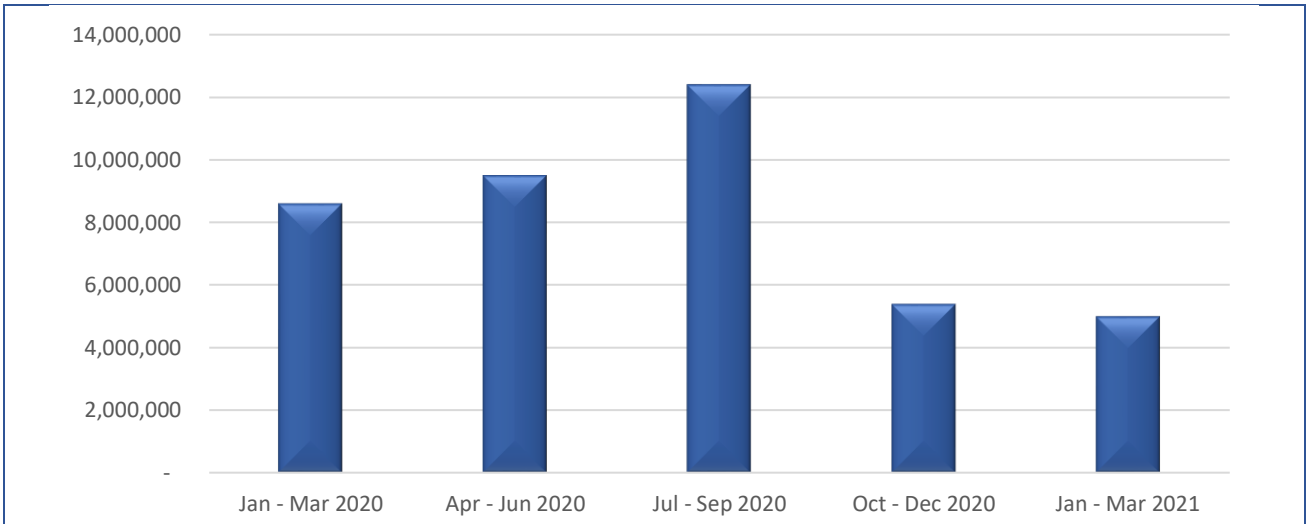
Source: Twitter

In terms of numbers, the second most troubling issue is related to **Child Nudity and Sexual Exploitation**. The spread of this type of online material is unfortunately still a huge problem today. In order to enforce a more effective fight against child sexual abuse, in July 2020, the European Commission published a Strategy to establish a comprehensive response both to offline and online child sexual abuse.

The EU strategy includes eight initiatives for the 2020-2025 period in order to put in place a strong legal framework, strengthen the law enforcement response, and facilitate a coordinated approach. One of the main goals involves proposing the necessary legislation to tackle child sexual abuse online by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities.

In terms of data, those released by Facebook show, fortunately, a decrease in the amount of content of this type which was intercepted (Fig.12). Between the first quarter of 2020 and the same period of 2021, child-pornography content removed dropped from 8.6 million to about 5 million (-41.9%).

Figure 12: Child Nudity & Sexual Exploitation content removed by Facebook



Source: Facebook

2.3 Online unfair business practices

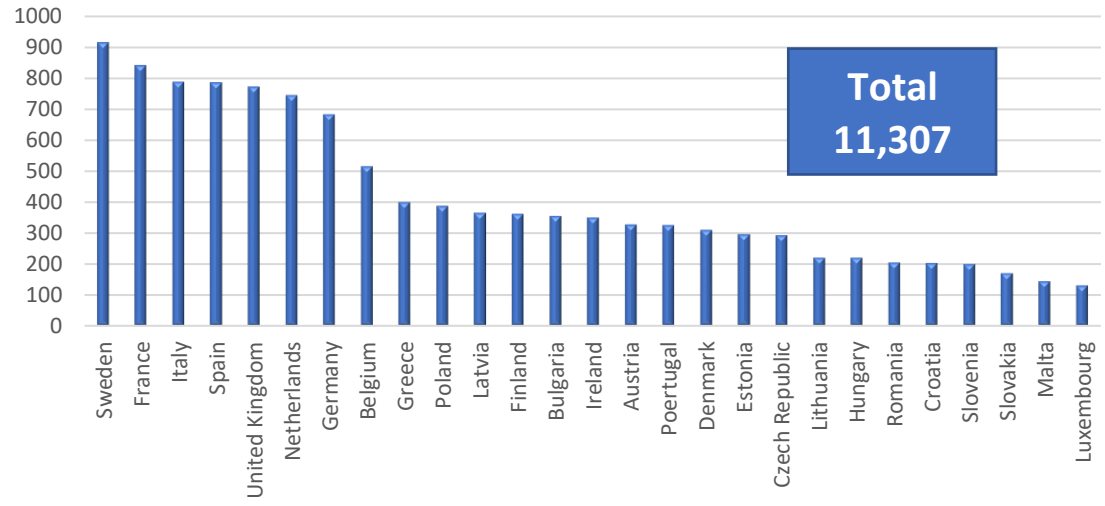
Besides malicious content, online platforms also monitor unfair business practices. **Online advertising** is constantly growing, and this implies that more people, as well as more "bad actors", are attracted by this trend and require further control by the platform in order to supervise and potentially **block unfair practices or real scams**.

This phenomenon has also intensified with the pandemic, where rogue traders started to advertise and sell products such as protective masks, caps and hand sanitisers that could allegedly prevent infection.
In March 2020, the consumer protection (CPC) authorities of the EU Member States issued the CPC Common Position COVID19 on the most reported scams and unfair practices identified, while the Commissioner for Justice and Consumers, Didier Reynders, wrote to the main digital players (social media, search engines and market places) in order to request their cooperation in tackling and taking down scams from their platforms.

Numbers provided by Twitter, Google and Microsoft provide an idea of the scope of this problem.

During the period considered - before the pandemic - the platform identified 11,307 ads promoting unacceptable business practices (Fig. 13).

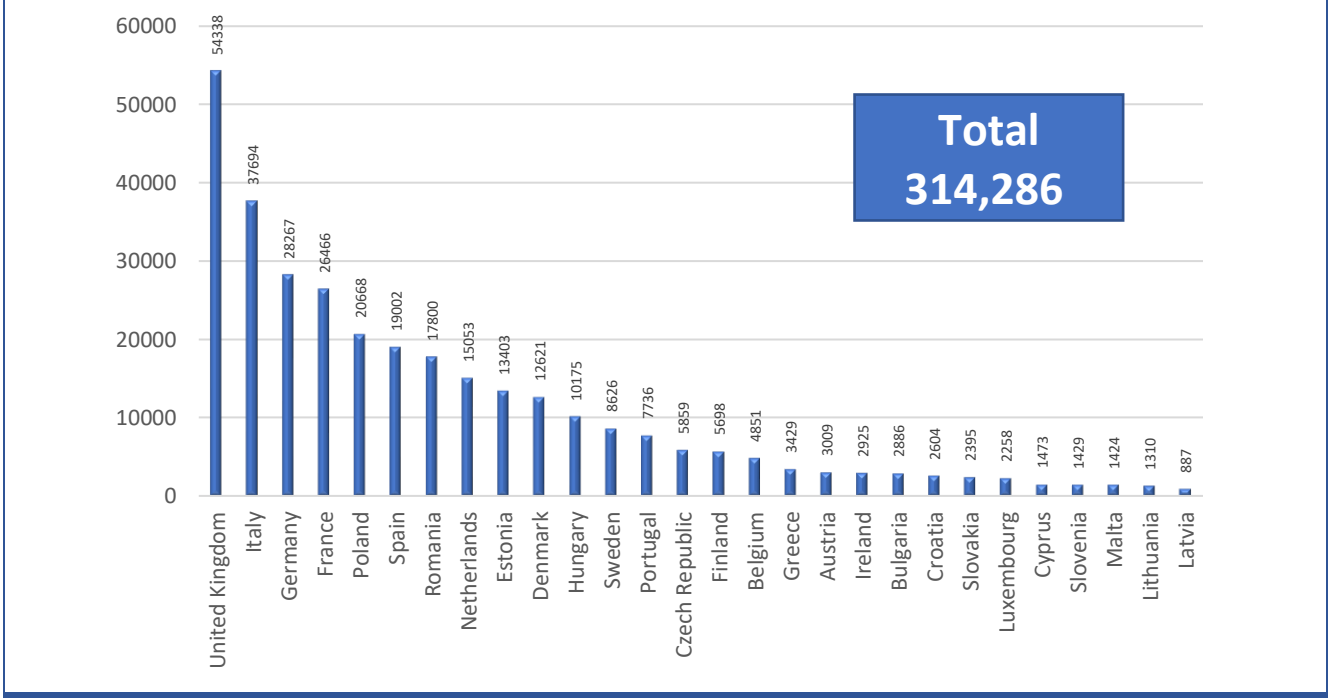
Figure 13: Unacceptable Business Practices in Ads rejected by Twitter (2019)



Source: Twitter

The high number of bad business practices carried out by companies in digital markets is also shown by data concerning violations of Google Ads accounts. To ensure that advertisers and publishers using their platforms comply with their policies, Google continuously monitors worldwide the advertising networks for compliance with these policies, using a combination of algorithmic and human reviews. Over one year, from September 2018 to August 2019, the total number of violations was 314,286 in the EU (Fig. 14). The Member State with the highest number of recorded violations was Italy (37,694), followed by Germany (28,267) and France (26,466). Instead, the country where Google registered the least number of violations was Latvia (877).

Figure 14: Google Ad accounts with misrepresentation policy violations (by billing country)



Source: Google, from 1 September 2018 to 31 August 2019

A similar trend was registered by Microsoft, as its Microsoft Advertising Service suspended nearly 200,000 accounts and removed 900 million bad ads and 300,000 bad sites in 2018. These figures represent removals based on all policy violations. Limited to misleading ads, Microsoft rejected more than 169 million ads between 1 July 2018, and 30 June 2019.

2.4 Fraud and counterfeiting activities in e-commerce space and consumer protection

E-commerce growth in responding to the pandemic resulted in an increasing number of consumers looking for less traditional ways of purchasing goods and services, mainly through online platforms. New user base entries also involved people not accustomed to using online services and, hence, less able to discriminate between good and bad listings on the platforms, making them an easy target for fraud and abuse. This also created favourable conditions for a parallel increase in bad actor attempts to take advantage of the growing digitalisation.

US data (Source: Federal Trade Commission) shows that American citizens have already lost more than $145 million to fraud related to COVID, measured by more than 200,000 complaints from

consumers, while Google identified a 250% increase in phishing sites between January and March 2020.

Marqeta's 2020 Fraud Report, which collects the interviews of 4,000 consumers across the UK and USA, shows that 42% of the sample had been hit by fraudsters. However, 63% of the same sample population said that they didn't accept it as inevitable and 87% of consumers stated they would be happy for transactions to take longer to complete, if extra steps for authentication meant their information was better protected.

However, the trade-off between a frictionless purchasing experience for the customer and the offer of a highly reliable protection system is not easy to manage. Still, even if facilitating consumer experience seems to be a primary need for merchants and e-commerce platforms, it is also true that the costs of frauds and scams in terms of revenue losses cannot be underestimated. According to a Signifyd's survey, 52.8% of consumers would tolerate no more than one negative experience with an online retailer before walking away for good, while only 8.9% would remain loyal to the retailer after the third scam.

Where e-commerce is concerned, malfeasance is of a different nature. The Account Takeover attacks (ATO), where identity thefts are used to gain unauthorised access to accounts, rose by 282% between 2019 and 2020. Chargebacks are very common, and they account for between 40% and 80% of fraud losses.

Phishing is used to steal payment information to make purchases through someone else's account. This type of fraud rocketed during the pandemic targeting non-tech-savvy people that approached digital services without being properly prepared. When it comes to e-commerce platforms, the range of possible malfeasances widens even more, as fraudsters introduce themselves into the systems by creating fake accounts and selling poor quality and counterfeit products.

The sudden increase in illicit acts has led to a transformation in how consumer protection is now handled. The trend is to shift from a defensive approach to risk intelligence models that work as a business optimisation engine. Because of the huge amount of data involved, protection systems may involve both human investigations and machine learning technology to process the huge quantity of information. As far as big platforms are concerned, they also contemplate the direct participation of seller partners in the evaluation.

The leading e-commerce platforms implemented a series of strategies in order to protect their customers.
For its part, Amazon has published the "Brand Protection Report" outlining its strategy to protect stores from fraud and abuse. Using both machine learning tools and human investigation, the company has built a system to check the identities of potential selling partners. Moreover, it has

developed the Payment Service Provider Program that forces operators to choose a provider which participates in the Program and, hence, is subject to specific requirements and compliance controls.

The company decided to engage directly with brand owners to improve the process of identifying bad actors and defending brand image and their intellectual property rights. To do this, it launched the Amazon Brand Registry, a tool through which partners can report suspected infringements. Furthermore, Amazon Transparency Services provide sellers with a system that protects the single product through the application of a 2D code that certifies the unit's authenticity. In addition, in order to pursue the zero-counterfeit objective, Amazon proposed the Zero Project, which involves automated processes that use the company's machine learning technology to identify bad actors and, at the same time, give sellers the power to directly eliminate risky listings from the store. In addition, the Amazon Counterfeit Crimes Unit aims at stopping bad actors to counterfeit products, holding them accountable through the court systems and criminal referrals and collaborating with law enforcement agencies around the world by building cases and undertaking independent investigations.

As for numbers, in 2020, the Amazon consumer base counted more than 300 million users and its network involved over 1.9 million selling partners worldwide. The company invested over $700 million in the protection of its stores and employed more than 10,000 people for this purpose. The size of the effort finds its rationale in the huge amount of attempted malfeasances carried out damaging to the company. In 2020, this verification blocked6 million actors that tried to create risky accounts, recording a dramatic increase in the number of aborted attempts, amounting to 2.5 million in 2019. Overall, only 6% of the new sellers attempting registration passed the verification tests. In 2020, 2 million products were seized and destroyed in warehouses because they were recognised as counterfeit. As a result, only 0.01% of the products sent to clients received complaints.

As far as the direct collaboration with brand owners is concerned, in 2020, the Brand Registry counted for over 500,000 brands enrolled that reported, on average, 99% fewer suspected infringements since enrolment. The Transparency Services were used in 2020 by over 15,000 brands resulting in the protection of more than 500 million product units. The number of brands participating in Project Zero is more than 18,000. It is important to stress that for every single listing removed by a brand through the self-service counterfeit removal tool, Amazon's automated protection removed more than 600 listings through scaled technology and machine learning. Regarding patent disputes, those handled through the company took on average 7 weeks, a lot less than the median time-to-trial for a U.S. patent lawsuit, which is 2.4 years.

Ebay, being a forum where sellers are connected to the buyer, has deployed Protection Programs for both kinds of actors. With the Buyer Protection Program, the company commits to intervening in disputes between buyers and sellers to rectify issues when the seller has failed to act adequately. Customers who take advantage of the programme usually receive a full refund, return the unsatisfactory product to the seller and are absolved from further obligations linked to the

transaction. On the other hand, through the Seller Protection Program, in order to protect sellers from abusive buyers, eBay discounts negative rating during disputes if the negative feedback in a protected sale is an isolated event, meaning that they won't count against the seller's performance status.

Zalando has adopted a strategy more focused on security and encryption. To combat the risk of data security breaches, the company relies on the encrypted transmission of customer data. This applies both to ordering and to registering for a customer account to prevent third parties from viewing the data. For this, the coding system SSL (Secure Socket Layer) is used. The company relies on special security technologies which constantly check the systems and identify and report anomalies to provide additional protection from external attacks. It also uses technical and organisational measures to secure the systems against loss, destruction, unauthorised access or distribution of customer data by unauthorised persons.

3. The new digital regulatory framework

The last twenty years have seen the growing emergence of digital services. A large number of digital platforms have accompanied and facilitated the transfer of many socio-economic activities into the network, increasing market efficiency, facilitating trade and innovation and providing enormous benefits to citizens, businesses and public administrations. This revolution has been accelerated by the pandemic that has forced the massive use of remote working and distance learning, encouraged the use of social networks and the enjoyment of online games and content demonstrating how the Internet and digital services have been representing the only real possibilities to ensure the continuity of services and guaranteeing of fundamental rights and freedom. Digital platforms are called upon here to even provide essential services.

This major acceleration along the path of digitalisation and the growing importance of intermediaries and platforms has called for a rethinking of their role and responsibilities and, therefore, of the relevant regulatory framework.

The new leadership of the European Commission, which took office at the end of 2019, immediately showed its awareness of this need. The guidelines for the period 2019-2024, published at the end of January 2020, and the digital strategy outlined in the Communication 'Shaping Europe's digital future', released on 19 February 2020, clearly expressed the Commission's desire to address the new opportunities and critical issues related to digitalisation and the new role to be played by intermediaries and platforms by defining new rules for digital services.

To this end, on 15 December 2020, the European Commission published a package including two legislative initiatives - the Digital Services Act (DSA) and the Digital Markets Act (DMA). In order to promote a maximum harmonisation within the EU and, thus, overcome the current regulatory fragmentation, the Commission has opted for directly applicable regulations instead of directives.

3.1 The DSA Proposal

The **DSA** amends, while maintaining its key principles, the E-commerce Directive (Directive 2000/31/EC), in order to ensure the best conditions for the provision of innovative digital services in the Internal market, contribute to online safety and the protection of fundamental rights (above all, freedom of expression and information) and establish a sound and sustainable governance model for the supervision of intermediary service providers.

The proposal is divided into **five chapters**, and has introduced a horizontal framework for all categories of content, products, services and activities on intermediation services. For the latter, however, a **diversified liability regime** is outlined on the basis of the services offered and the size of the supplier (e.g. some obligations are limited only to very large online platforms, which have acquired a central and systemic role due to their scope). The same proposal places **specific obligations on the Member States** to verify the compliance of these subjects operating in their

respective territories relative to the provisions contained in the proposed regulation, also establishing new subjects (Coordinators for Digital Services) and defining mechanisms of enforcement and cooperation between the states.

A) Categories of providers and liability exemptions

The proposal identifies several types of providers, namely:

a) **"mere conduit" services (art. 3),** which consist of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network. The service provider is not liable for the information transmitted, on condition that the provider does not initiate the transmission, does not select the receiver of the transmission and does not select or modify the information contained in the transmission.

These service providers will not be liable for the information transmitted when they do not initiate transmission, do not select the recipient of the transmission and do not select or modify the information to be transmitted. This includes the automatic and transient storage of the information transmitted in so far as this is necessary for the transmission and does not exceed the time reasonably required for transmission;

b) **"caching" services (art. 4)** which consist of transmitting, over a communications network, information provided by a recipient of the service, by means of the automatic, intermediate and temporary storage of that information carried out for the sole purpose of making more efficient the subsequent forwarding to other recipients at their request. In such cases, the provider is not liable for the content entered by others if: (i) it does not modify the information; (ii) it complies with the conditions of access to the information; (iii) it complies with the rules for updating the information, according to the rules of the industry; (iv) it does not interfere with the lawful use of technology recognised and used in the industry to obtain data on the use of the information; (v) acts promptly to remove the information it has stored, or to disable access to it, upon obtaining actual knowledge that the information has been removed from its initial location on the network or that access to the information has been disabled or that a court or administrative authority has ordered its removal or disabling. The provision specifies that the judicial authority or the administrative authority with supervisory functions may require, also as a matter of urgency, that the provider, in the exercise of the aforementioned activities, prevent or put an end to the violations committed;

c) **"hosting" services (art. 5)** that consist of the storage of information provided by a recipient of the service where the service provider is not liable for the information stored at the request of a recipient of the service on condition that the provider does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent or, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.

Where the provider voluntarily implements activities aimed at detecting, identifying and removing, or disabling access to illegal content, or adopts the necessary measures to comply with the EU regulatory framework, does not constitute a cause for forfeiture of the exemptions of liability

described, while the provision of general monitoring or investigation obligations on providers is expressly excluded.

B) Due diligence obligations

The proposed regulation imposes **different due diligence requirements**. In particular, the regulation requires **all providers of intermediation services, regardless of size and the service offered**, to establish a **single point of contact** for direct communication with the authorities of the states; the identification, for providers not established in the EU, of a **legal representative in one of the Member States** in which it offers its services; the inclusion in **clear and accessible language** in its terms and conditions, of information concerning any restrictions imposed on the use of the service, including those relating to policies, procedures, measures and tools used for the **moderation of content**, including the algorithmic decision-making process employed and the publication, at least once a year; of **reports** (ex art.13), easily understandable and detailed on any moderation of content undertaken by them in the reference period (with specific information including the number of measures received by the authorities of the Member States, divided on the basis of the type of illegal content to which they relate, with an indication of the average time required to take the required action).

In addition to these general provisions, the proposal introduces specific provisions for certain types of providers. As regards, in particular, providers of hosting services, including online platforms, the regulation provides for the establishment of **notification and action mechanisms** that allow individuals and entities to report the presence of illegal content, providing a series of information (including the precise indication of the URL or URLs) against which the same provisions configure precise obligations of feedback (also defining the information to be transmitted in the feedback) and the sending of a **detailed and reasoned information** to the recipients of the service about the decision to remove or disable access to certain information (the decisions taken and the relative reasons in support will be published in a public database managed by the Commission).

With regard to **online platforms (with the exclusion of platforms qualified as micro or small enterprises),** the proposed regulation prescribes:

(a) the provision of an **internal system for handling complaints** against decisions to remove or disable access to information, suspend or interrupt the provision of the service, in whole or in part, to recipients and suspend or close the recipients' account. Complaint management requires the use of timeliness, diligence and objectivity, prompt communication of the decision taken on the complaint received and, if the complaint is well-founded, prompt revocation of the decision;
(b) the **possibility for the recipients of the service to appeal to an out-of-court dispute resolution body** (the certification of the possession of the requisites is entrusted to the Coordinator of the Digital Services of the Member State in which the body is established,

while the list of bodies is published and updated by the Commission on the basis of the lists provided by the Coordinators). The same provision regulates the issue of the costs relating to the procedure, providing for the reimbursement by the platform in the event it loses the case, but not providing for the same obligation to be borne by the recipient of the service in case of his/her defeat;

(c) the provision of technical and organisational measures to ensure that warnings coming from "**trusted reporters**" are processed and decided on a priority basis (meaning persons meeting specific requirements verified by the Digital Services Coordinator, who confers - and possibly revokes - such status);

(d) the provision of **measures and protection against abuse**. Platforms are granted the possibility, on the basis of a set of circumstances to be verified, to suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients who provide manifestly illegal content and to suspend the notification mechanism and the internal complaint handling system for persons or entities that have frequently submitted manifestly unfounded reports or complaints;

(e) the **notification of suspected offences.** Obligation to promptly inform, for platforms which have learned of information giving rise to suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place, the law enforcement or judicial authorities of the Member State or States concerned;

(f) the **traceability of sellers**. The regulation identifies the information that the platforms that allow consumers to conclude distance contracts with sellers must obtain, placing on the same platforms the burden of verifying, making reasonable efforts, the reliability of the information received through the use of official online databases that are freely accessible or through the online interface made available by a Member State or by the Union, or through the request to the trader to provide supporting documents from reliable sources, as well as the power to suspend the service to the seller until the latter fulfils its information obligations. This information must be retained for the duration of the contractual relationship with the seller and must be deleted if the relationship is terminated;

(g) the **respect of transparency obligations**. The report foreseen for all providers is enriched, in the case of platforms, by additional information relating to the activity of internal complaint management systems and out-of-court dispute resolution bodies, as well as information relating to the number of average monthly active users in each Member State which platforms must publish and communicate to the Digital Services Coordinator at least once every six months;

(h) **transparency of online advertising**. Art. 24 requires online platforms that display advertising on their online interfaces to ensure that users can identify, for each specific ad displayed, clearly and unambiguously and in real time, that the information displayed is an advertisement, the natural or legal person on whose behalf the ad is displayed and meaningful information about the main parameters used to identify the recipient of the advertisement.

Additional obligations are imposed on **large platforms identified as having at least 10% of the EU population (45 million users),** which are required to:

(a) carry out an **annual risk assessment** to identify and analyse possible systemic risks deriving from the use of their services within the EU and prepare the relative mitigation measures (the proposal foresees the adoption by the Commission, in cooperation with the Coordinators for the Digital Services, of specific guidelines);

(b) undergo, at its own expense, an **audit at least once a year** by an independent organisation to verify compliance with the obligations incumbent on it and draw up a report (drawing up, in the event of any criticalities detected, within one month of receiving the recommendations aimed at overcoming them, a report where to give an account of the measures adopted or the reasons that led to the adoption of different measures);

c) with regard to **online advertising**, maintain and make public (for at least one year from the last time the advertisement was displayed) a file containing information relating to the content of the advertisement, the natural or legal person on whose behalf the advertisement is displayed, the period during which the advertisement was displayed, whether the advertisement was intended to be displayed specifically to one or more specific groups of users of the service and, if so, the main parameters used for this purpose and the total number of users reached;

d) allow the Commission and the Coordinator **access to the data**, following a specific request and for a reasonable period of time indicated in the same request, for the purposes of verifying compliance with the obligations set out in the Regulation. The same obligation to disclose data will apply to researchers - affiliated with academic institutions, with proven expertise, independent of commercial interests and able to ensure data security - for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks. It will be up to the Commission to define the technical conditions under which data may be shown and the purposes for which such data may be used;

e) identify its own **compliance officers** (to be communicated to the Commission and the Coordinator), responsible for verifying compliance with the provisions contained in the Regulation, collaborating with the Commission and the Digital Services Coordinator, organising and supervising the activities relating to the audit and informing the managers and employees of the platforms about the obligations provided for by the Regulation;

f) transmit, in addition to the reports foreseen for the other suppliers, to the Commission and the Coordinator, a **report** containing the risk assessment and the relative risk mitigation measures, the audit report and the report on the implementation of the measures requested during the audit.

The proposal also encourages the development of **Codes of Conduct** that set objectives to be pursued, identify performance indicators in relation to the achievement of these objectives - which the Board, bringing together the Coordinators, will monitor - and take into account the interests of all stakeholders, including citizens, at EU level. The adoption of Codes of Conduct is also encouraged with regard to online advertising in order to ensure adequate protection of the rights of all stakeholders and the establishment of a competitive, transparent and fair environment for online advertising.

C) Governance structure and penalties

In defining the **structure of governance**, the proposed Regulation requires Member States to identify **one or more authorities responsible for the application of the Regulation** and of a **Coordinator for the Digital Services to** identify the requirements and the powers of inspection, imposition and sanctioning, and make it responsible for all the questions connected to the application and the enforcement of the Regulation within the state. Moreover, it would be called on to cooperate with the other national authorities, with the Commission and the European Board for the Digital Services (instituted by the Regulation and made up of the representatives of the Coordinators) and to draw up and transmit to the latter an annual report.

The same regulation also describes the **cooperation procedures** for the Coordinators, regulates the modalities through which joint investigations can be carried out and provides for the possibility of activating the **investigative and enforcement powers of the Commission** in the case of suspicion of violation of the Regulation by the large platforms. With regard to the violations committed by the large platforms, in particular, the Regulation outlines a structured procedure in which the Commission, the Board and the Coordinator are called upon, each within their own sphere of competence, to express their opinion on the action plan proposed by the platform in order to assess the adequacy of the measures proposed to put an end to or remedy the violation. The Regulation establishes the criterion to be followed to identify the **jurisdiction**, connecting it to the Member State where the supplier's head office is located, while for suppliers not established in the Union, the Member State where the legal representative is established will have jurisdiction.

In order to manage possible crisis situations caused by extraordinary circumstances affecting public safety or health, the proposal foresees the possibility for the Commission to proceed to drawing up **crisis protocols** - through the involvement of platforms and possibly also Member States' authorities, the Community institutions and civil society organisations - setting out the parameters for determining the existence of a crisis situation, the objectives, the measures to be implemented and the role of the various actors involved, the definition of a clear procedure for identifying the period of implementation of these measures, the provision of forms of publicity regarding the measures adopted, the reference period and the results obtained at the end of the crisis.

In order to ensure compliance with the provisions of the Regulation, the proposal provides for the possibility for Member States to provide for **penalties** of up to 6% of the annual turnover of the supplier (1% in the case of non-compliance, e.g. failure to submit to inspection, failure to respond to requests for information, etc.).

The DSA proposal will bring about important changes, redesigning the role and responsibilities of platforms and producing a strong impact on platforms. The new regulatory framework proposed

has been triggering a wide debate among stakeholders summarised also by the European Parliament in its briefing on the Commission's proposal.

On 28 May 2021, MEP Christel Schaldemose submitted her draft report on the Digital Services Act (DSA) to the European Parliament's Internal Market and Consumer Protection Committee (IMCO).

The Report welcomes the Commission's proposal on a Digital Services Act. However, it proposes several amendments. Amongst the most significant are:

1) **Online marketplaces.** Stricter rules should be introduced in order to create a level playing field and ensure the principle, stated by the European Commission, of "what is illegal offline should also be illegal online". A new article, laying down stricter conditions for liability exemptions specifically targeting online marketplaces, is proposed. These conditions include requirements to comply with certain due diligence obligations and conditions that ensure that where a trader from a third country does not have an economic operator liable for the product safety, the marketplace will not benefit from the exemption of liability. As well, the obligation on the traceability of traders has been strengthened by introducing a new article extending the scope of certain provisions presented in Article 22 to all intermediary services and by introducing new provisions targeting online marketplaces. These provisions include obligations to prevent dangerous and/or non-compliant products from being offered online and obligations to cooperate with national authorities, when necessary, regarding dangerous products already sold.

2) **Removal of illegal content.** The report states that illegal content should be removed from intermediary services as fast as possible while taking into account fundamental rights. Therefore, the DSA should establish a framework for notice and takedown with clearly defined procedures, safeguards and timelines for acting on notifications on illegal content and ensure uniform procedures in all Member States. While it is necessary to grant digital platforms time to assess the legality of content, some content has a very high impact and may pose a greater threat to society or important damage to the individual. The report favours two sets of timelines with shorter timeframes for such high impact content.

3) **User rights.** The Report welcomes the Commission's proposal for an internal complaint-handling system and the out-of-court dispute settlement body. However, in order to ensure an efficient procedure, it wants timeframes to be included. In addition, the internal complaint-handling system should not only be available for those whose content has been removed, but also for those whose notification has been rejected. Moreover, not only national authorities and the Commission should have access to direct and efficient means of communications with intermediary services, but also the recipients of services. The Report proposes a new Article that allows recipients of services to choose between means of communication with the intermediary services. Lastly, according to the Report, the

additional obligations imposed on online platforms under the Regulation's Chapter two, Section three, should be applicable to micro and small enterprises as well (Transparency reporting obligations for providers of online platforms). Consumer protection law does not differentiate between small and big enterprises and, therefore, the obligations should not be limited to larger platforms.

4) **Online advertising.** The Report affirms that transparency alone cannot solve the problems related to targeted online advertising. Therefore, it proposes a new article to allow consumers to navigate through online platforms without being subject to targeted advertising, providing for targeted advertising to be set off by default and for consumers to be able to easily opt-out. The Report also suggests that when online intermediaries process data for targeted advertising, it cannot carry out activities leading to pervasive tracking. Furthermore, it proposes to extend the scope of the article on online advertising transparency to all intermediary services and suggests new transparency provisions, such as specifying the person who finances the advertisement and where the advertisement has been displayed. Moreover, the intermediary service should allow access to NGOs, researchers and public authorities upon their request to information on direct and indirect payment or any remuneration received. Lastly, in order to improve consumer awareness of commercial content, the Report suggests to have prominent and harmonised markings of advertisements. Today, it is up to the individual trader to decide how to disclose the advertisement as long as this is judged as being sufficiently clear to an average consumer of the expected target group. This freedom results in a variety of different markings which makes it difficult for consumers to recognise an advertisement. Therefore, the Report affirms that a prominent and harmonised marking for advertisements would be needed.

5) **Recommender systems and algorithmic accountability.** The Report sees the need to further strengthen the empowerment of consumers when it comes to recommender systems. First of all, it suggests to extend the scope of the article to all online platforms as recommender systems used on platforms with less than 45 million active users also have a significant impact on users. Furthermore, it proposes that any recommender system should, by default, not be based on profiling, and that consumers subject to recommender system using profiling should be able to view and delete any profiles used to curate the content they see. In addition, the Report believes that the algorithms used in recommender systems should be designed to prevent dark patterns and rabbit holes from happening. Moreover, a "must-carry" obligation to ensure that information of public interest is high-ranked in the platform algorithms is proposed. Lastly, the Report finds that greater accountability on algorithms should be introduced in the proposal, enabling the Commission to assess the algorithms used by very large online platforms and determine whether they comply with a number of requirements. The Commission would be allowed to impose sanctions in the case of infringement of certain requirements.

6) **Implementation and enforcement**. Taking inspiration from Regulation (EU) 2017/2394, the Report proposes that the Digital Service Coordinator and the Commission should be able to restrict access to the interface of an intermediary service, if the provider repeatedly infringes the Regulation's obligations. Furthermore, the Commission should not only be able to act, but should also be obliged to act if it has reasons to believe that a very large online platform has infringed the Regulation.

3.2 The DMA Proposal

The impressive dynamism, together with the ability of new players to achieve market dominance positions within a few years, are elements of great change compared to the workings of the "traditional" markets of the past.
To provide an answer to the new critical issues connected to the affirmation of large online intermediaries and platforms, the European Commission proposed the Digital Market Act (DMA) which represents one of the most important milestones of the EU digital strategy.

The proposal for a regulation on digital markets, starting from the observation of the ever-increasing importance of digital services for the performance of daily activities and their extraordinary contribution in terms of increasing choice for consumers, the efficiency and competitiveness of the industry and the presence in the market of a small number of large platforms with an extremely high market share, has established a series of strictly defined objective criteria to qualify a large online platform as a gatekeeper and places, according to an ex ante approach, a series of obligations and prohibitions on these entities.

The Commission's choice has been to provide for ex ante rules through the adoption of a regulation and, therefore, an instrument of **maximum harmonisation**. This choice reveals some opportunities but also potential criticalities. In fact, the prevision of ex ante rules could potentially accelerate authorities' intervention and the collection of more data on possible anti-competitive conduct, limiting or even preventing the damage of anti-competitive conduct, ensure greater transparency and detail on the functioning of the digital marketplace and the platforms that operate within it and facilitate targeted intervention on gatekeepers. At the same time, however, ex ante regulations may not be very adaptable and flexible in a digital marketplace undergoing rapid and continuous change representing a real threat to suppress innovation and competitiveness in Europe.

Therefore, the proposed regulation is aimed at those platforms that increasingly act as gateways or gatekeepers between commercial users and end users, hold an established and long-lasting position and the power to make improper use of user data, reinforce barriers to market entry and engage in misconduct towards commercial users and end users. The scope of this regulation is focused on 8

"core platform services"[11]: online B2C intermediations services; online search engines; social networks; video sharing platforms; number-independent interpersonal communication services; operating systems; cloud computing services; and advertising services, including any advertising networks, advertising exchanges and any other advertising brokerage services, provided by a provider of any of the above services.

For the purposes of defining the prerequisites for qualifying a provider as a gatekeeper, the proposed regulation requires (art. 3) the following conditions:
1) **significant impact on the internal market**, which is presumed whenever the undertaking has had an annual turnover in the European Economic Area of at least €6.5 billion during the last three financial years (or where the average market capitalisation was at least €65 billion during the last financial year) and offers the service in at least three Member States;
2) **important gateway to reach end-users**, which occurs when the provider connects a large user base to a large number of businesses (specifically more than 45 million monthly active end-users established or located in the Union and more than 10,000 active business users per year established in the Union in the last financial year);
3) **possession (or foreseeable possession in the near future) of an entrenched and durable position in its operations.** This requirement is deemed to be met when the thresholds referred to in point b) have been reached in each of the last three financial years.

The possession of these requirements determines the provider's obligation to notify the Commission, although the Commission has the power, independently, to identify as a gatekeeper the provider who fails to comply with this notification obligation. In addition, the Commission would have the power to review the gatekeeper status of a particular ISP in the event of a material change in the basis for the gatekeeper decision, or if the gatekeeper decision was based on incomplete, incorrect or untrue information. In general, the proposed regulation requires the Commission to verify, at least every two years, whether gatekeepers are meeting the requirements of the regulation and whether additional providers are meeting those requirements.

Specifically, art. 5 sets several obligations and prohibitions on gatekeepers, which will **have to**:
a) allow third parties to inter-operate with the gatekeeper's own services in certain specific situations;
b) allow their business users to access the data that they generate in their use of the gatekeeper's platform;
c) provide companies advertising on their platform with the tools and information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper;

[11] Seven principal and one accessory (advertising services which will be regulated only when offered by a provider of any of the principal CPS).

d) allow their business users to promote their offer and conclude contracts with their customers outside the gatekeeper's platform;
e) ensure the effective portability of data generated through end-user or business activity.

Instead, these platforms will be **prohibited to**:
a) treat the services and products offered by the gatekeeper itself more favorably than similar services or products offered by third parties on the gatekeeper's platform;
b) forbid consumers from connecting with businesses hosted outside of gatekeeper platforms;
c) prevent users from uninstalling any pre-installed software or applications if they so desire;
d) use business users' data for the purpose of competing with them.

The proposal introduces the possibility to **exceptionally suspend in whole or in part a specific obligation** - adopting a specific decision at the latest 3 months following receipt of a complete reasoned request - when the gatekeeper demonstrates that compliance with that specific obligation would endanger, due to exceptional circumstances beyond the control of the gatekeeper, the economic viability of the operation of the gatekeeper in the Union, and only to the extent necessary to address such a threat to its viability (art. 8).

The proposal also sets a broad obligation on gatekeepers to inform the Commission of *"any intended **concentration** involving another provider of core platform services or of any other services provided in the digital sector"* (art. 12) and the submission to the Commission, within six months of their designation as gatekeepers, of a description, verified by an independent party, of all **consumer profiling techniques** that the gatekeeper applies to or through its services (art. 13).

Aware of the speed of technological change, the Commission provides the possibility to conduct a **market investigation** with the purpose of examining whether one or more services within the digital sector should be added to the list of core platform services or to detect types of practices that may limit the contestability of core platform services or may be unfair, and which are not effectively addressed by this proposal.

The proposed regulation defines in detail the **powers of the Commission**, granting it the power to request information, conduct inspections, order interim measures, make binding commitments proposed by the gatekeeper, carry out monitoring activities regarding compliance with the obligations under the proposed regulation, adopt decisions certifying infringements by gatekeepers and impose **penalties.** The latter, in particular, are quantified up to 10% of the total annual worldwide turnover of the company. Moreover, systematic violation of the regulations may lead to the application of extraordinary **structural remedies** such as the obligation to sell part of the company's assets or property (splitting).

In carrying out the activities regulated by the DMA, the Commission is assisted by the Digital Markets Advisory Committee.

Commission decisions and sanctions imposed by the Commission are subject to the jurisdiction of the European Court of Justice, which may cancel, reduce or increase them.

On 10 February 2021, the **European Data Protection Supervisor** (EDPS) adopted an **opinion** on the Digital Markets Act (and on the Digital Services Act).
Welcoming the European Commission's proposal and the goal to promote fair and open digital markets, the EDPS underlines the importance of guaranteeing the fair processing of personal data by regulating large online platforms acting as gatekeepers.
Specifically, the EDPS highlights, on the one hand, the importance of fostering competitive digital markets ensuring individuals a bigger choice of online platforms and services that they can use, and on the other hand, emphasising the necessity to give users better control over their personal data. The EDPS also underlines that increased interoperability can help to address user lock-in and ultimately create opportunities for services to offer better data protection.
Finally, the EDPS encourages a closer cooperation between the relevant supervisory authorities, including data protection authorities, consumer protection authorities and competition authorities to guarantee the successful implementation of the European Commission's Digital Services Act package.

The proposal launched by the Commission is triggering a wide-ranging debate.
In general, **BEREC (**Body of European Regulators for Electronic Communications) has welcomed the proposed ex-ante regulations but, at the same time, has underlined the risk that the provision of obligations built mainly around practices that have already been identified or investigated in the past, may be unable to keep up with the rapid technological changes. For the governance, BEREC has proposed the attribution of implementation and enforcement powers to national authorities and the provision of the possibility for the competent authorities to tailor remedies on a case-by-case basis and provide such authorities with the appropriate mandate to collect relevant data from gatekeepers and market players and continuously and actively monitor the digital services. BEREC has also proposed the establishment of an independent advisory board of national authorities to improve coordination and harmonise national authorities' actions and the provision of a dispute resolution mechanism.

On 1 June 2021, MEP Andreas Schwab submitted his draft report on the Digital Markets Act (DMA) to the European Parliament's Internal Market and Consumer Protection Committee (IMCO).

The Report welcomes the European Commission's proposal, suggesting the following main modifications:

1) Definition and designation of gatekeepers. The Report believes that the DMA should clearly target those platforms that play an unquestionable role as gatekeepers due to their size and their impact on the internal market. To this end, the Report deems it appropriate to increase the quantitative thresholds and to add - as an additional condition for companies to be designated as

gatekeepers under Article 3(2) of the Regulation - that they are providers of not only one but, at least, two core platform services. The provision of two or more core platform services is also an important indicator of the role of these companies as providers of service ecosystems. These changes should not preclude the Commission's ability to designate as gatekeeper other providers of core platform services, following an assessment under Article 3(6). At the same time, such a thorough analysis should not be required (nor would it be justified) where companies meet the quantitative thresholds of Article 3(2). The Report would like the application of this Regulation to be fast and efficient. Companies are therefore expected to cooperate but if they do not, the Commission should be able to designate a provider of core platform services as a gatekeeper based on the facts available. At the same time, legal predictability should be enhanced. To this end, the Rapporteur proposes a list of indicators to be added as an Annex to this Regulation, in order to enable providers of core platform services to know in advance how to establish the number of monthly active end-users and yearly active business users for the purposes of Article 3(2).

2) Obligations and prohibitions. The Report notes that a different clustering of the obligations and prohibitions could have brought added value to this Regulation. Nevertheless, the Report also sees merit in the segmentation proposed by the Commission, which identifies the obligations susceptible of being further specified, to the benefit of an effective application of the Regulation. The Report suggests further changes to be made, clarifying that the obligations and prohibitions foreseen in the Regulation are self-executing, and that gatekeepers are expected to ensure compliance as soon as the Regulation enters into force. Furthermore, the Report is of the view that the regulatory dialogue should foresee the possibility for the Commission to market-test the measures the gatekeeper is expected to implement in order to ensure effective compliance with the Regulation. Moreover, the Report proposes that the anti-circumvention prohibition should be strengthened to prohibit gatekeepers from engaging in any behaviour that would, in practice, have the same object or effect as the practices listed in Articles 5 and 6.

3) Market investigation and structural remedies. The Report asks the Commission to be allowed to request national authorities to support market investigations for the designation of gatekeepers. In addition, the imposition of structural remedies should be possible after the adoption by the Commission of two non-compliance decisions. The Report holds that such an approach is justified given the ex-ante self-executing nature of the Regulation. For the same reason, the adoption of commitment decisions should not be possible.

4) Governance, enforcement and regulatory consistency. Given the nature of digital services means that different regulatory regimes will inevitably interlink and overlap, the Report proposes the creation of a High Level Group of Digital Regulators, bringing together representatives of the competent authorities of all Member States, the Commission, as well as any relevant EU bodies and other representatives of competent authorities in specific sectors. Such a High Level Group should facilitate cooperation and coordination between the Commission and Member States in their enforcement decisions, in the interest of a consistent regulatory approach. The High Level Group

should also assist the Commission in monitoring compliance with this Regulation by enabling the pooling of insight, resources and expertise across Europe to the benefit of EU consumers and the internal market.

The Report's proposals partly align with the content of the non-paper released by the governments of France, Germany and the Netherlands at the end of May. The so-called "Friends of an effective Digital Markets Act" claim that the scope of the DMA should be targeted, taking the role of ecosystems into account more explicitly. They stress how, aside from safeguarding fairness for users of gatekeeper platforms, the DMA is aimed at preserving market contestability. A greater role should be envisaged for Member States to set and enforce national rules including national competition law, request a market investigation not only under art. 15 but also under art. 16 and art. 17, and support the Commission's enforcement capacity, thanks to national authorities.

Moreover, the non-paper call for the setting up of a steering group to ensure coordination and cooperation (that could resemble the High Level Group, proposed by Mr. Schwab), the private enforcement of the gatekeeper obligations and the enhancement of art. 12 (obligation to inform about concentrations), modifying the merger control system under Regulation (EC) No. 139/2004. According to the non-paper, the current text of art. 12 lacks ambition while it should foresee setting clear and legally certain thresholds for acquisitions by gatekeepers of targets with relatively low turnover but high value, and adapting the substantive test to effectively address cases of potentially predatory acquisitions.

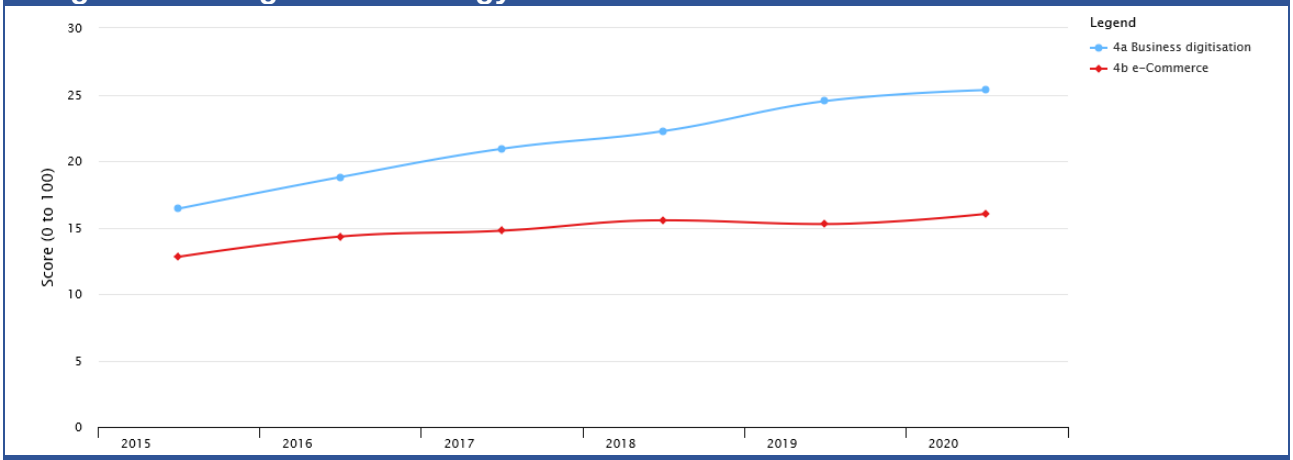
4. Economic effects from the DSA package

Following the introduction of the new legal framework that was introduced with the Digital Services Act package, which includes the Digital Services Act (DSA) and the Digital Markets Act (DMA), a multi-dimensional policy discussion has ensued. There are many different aspects and topics covered by the new legislation. The DSA package implementation is recognised as an important new policy element that will trigger various direct and indirect effects in the wider business ecosystem – across different sectors and not just platforms - and the European economy. Following the pandemic crisis, the introduction of new digital technologies and the emergence of new business models have rapidly emerged and are currently reshaping the business environment in the post-pandemic era. This fast digital transition has created new societal and regulatory challenges and is currently outpacing an outdated EU regulation with the corresponding directives regarding digital services still aligned with the original e-Commerce Directive introduced in 2000. The reconstruction and updating of the current regulation and the introduction of novel directives to cover emerging aspects that had been previously disregarded is imminent. On the other hand, regulatory intervention should be designed cautiously as over-regulation in digital markets is bound to have counter-effects and affect the market's functionality. In this chapter, we briefly explore the impact and ramifications of the introduction of the DSA package in three different dimensions: a) the impact on business ecosystems with a special focus on Small-Medium Enterprises (SMEs); b) the effects on the competition in the Digital Single Market; and c) the broader impact of this new regulatory package on overall competitiveness and innovation.

4.1 Impact on businesses ecosystems with a special focus on SMEs

The revision of the outdated legal landscape of EU digital space was indeed required after almost 20 years. The world of the "worldwide web" has changed, as new businesses have emerged, new media created and new mechanisms and tools of doing business introduced in every sector of the economy. The majority of firms are reshaping and digitalising many of their activities. On the other hand, online markets are no longer complementary sources of revenues and are quickly emerging as the primary source of income. **Error! Reference source not found.**6 shows that EU performance regarding Business digitalisation and e-Commerce has improved over the last five years. The empirical data presented in Figure 16 is drawn from the Digital Economy and Society Index (DESI). A closer look at the Figure reveals an increasing pattern for Business digitalisation. More specifically, the index improved from 16.4% in 2015 to 25.3% in 2020. A similar pattern is also seen in the e-Commerce index, although to a lesser degree. The performance of e-Commerce improved on a lower scale (from 12.8% in 2015 to 16.0% last year).

Figure 16: DESI index, Integration of Digital Technology, by Sub-dimensions of 4 Integration of Digital Technology



Source: European Commission

In addition to the positive market trends, the COVID-19 pandemic has amplified the importance of digitalisation and created new opportunities for businesses to retain their market position and resilience and, in some cases, even improve their positioning and regain a competitive advantage. It may have served as a defensive strategy at the beginning in order to cope with the obstacles created by the pandemic, but it was soon realized that elements of this strategy should be formulated to last longer than originally expected.

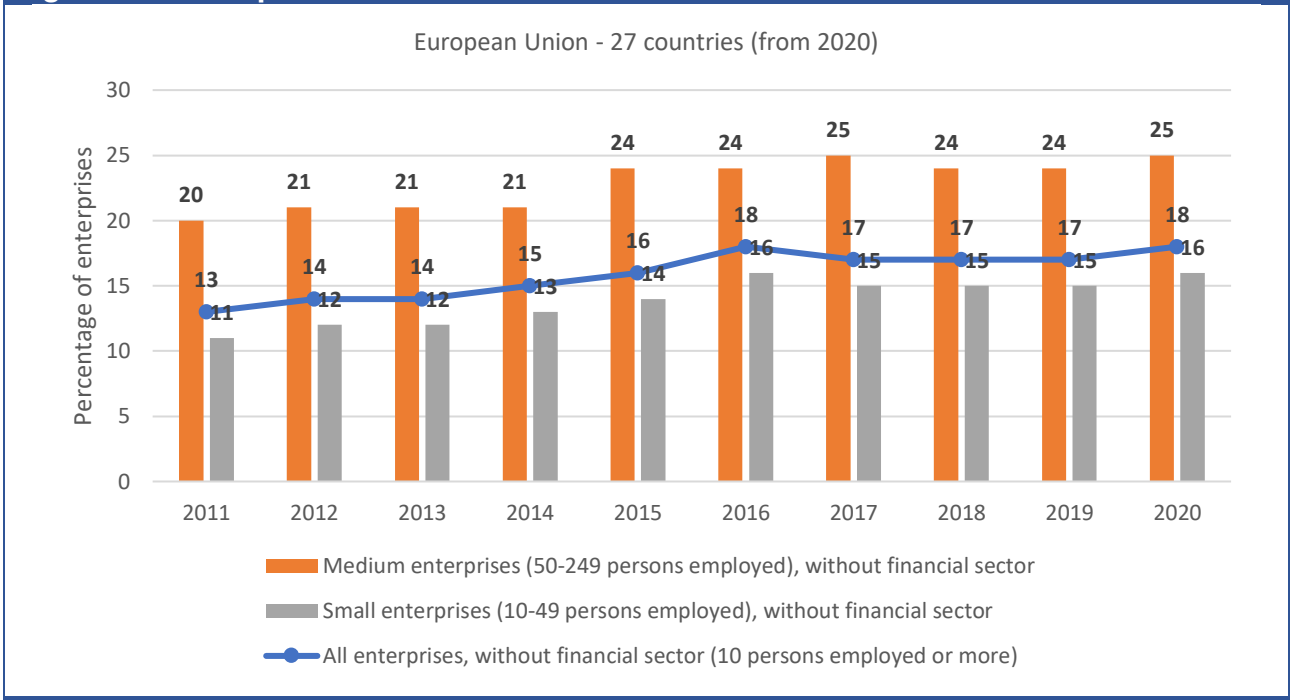
From a different perspective, the emergence of digital markets presents fertile ground and opportunities for new business ventures, as well as the improvement and expansion of already established actors. When focusing on SMEs, the vast majority of enterprises in the EU (approximately 99% of all enterprises), a new reality of a single EU digital market could foster a wave of positive spillovers. A glance at some structural statistics indicates that SMEs employ around 100 million people, account for more than half of Europe's GDP and play a key role in spreading innovation throughout Europe's regions[12].

However, according to Figure 17, the increasing trend of e-commerce in the last ten years has mostly benefited medium-sized enterprises that have secured higher shares in e-commerce sales out of their total turnover compared to SMEs, in general. A closer look at the most recent data (2020), reveals that the e-commerce sales share of SMEs was approximately 16% compared to a 25% share for medium enterprises. At the aggregate level, EU enterprises with at least 1% of their turnover deriving from e-commerce sales accounted for 18% of total enterprises in 2020, greatly improving on their respective share (13%) in 2011. When accounting for size, medium enterprises systematically score higher sales shares than SMEs in the examined period. This data indicates that firm size is closely correlated to the success in digital markets. Considering the fact that SMEs

[12] https://ec.europa.eu/growth/smes_en

outnumber the rest of the size categories in the EU, the facilitation of an EU Single Market is an essential venture to improve the overall EU performance in digital markets.

Figure 17: Enterprises with e-commerce sales of at least 1% turnover

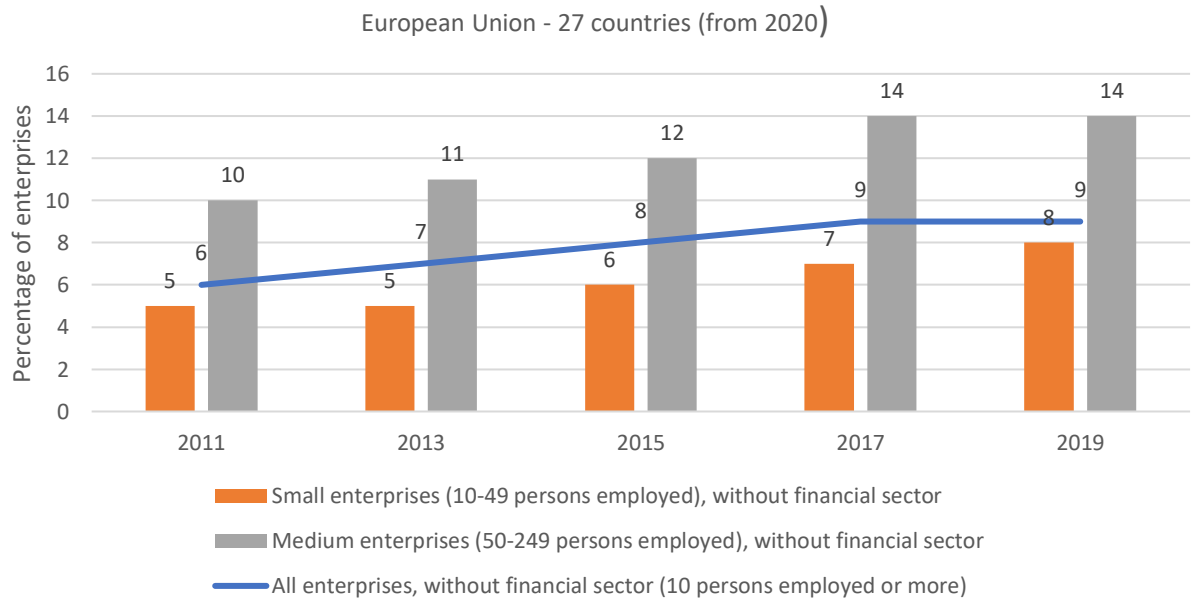


Source: European Commission

One of the main targets of the newly introduced directives is to support cross-border sales by decreasing the costs of complying with possibly 27 different business regimes. This targeted harmonisation across Member States is critical for the proper function of the EU Single Market since complying with regulatory and administrative requirements is challenging for growing businesses, particularly in the context of cross-border activities. **Error! Reference source not found.** illustrates data regarding the difficulty of SMEs expanding their sales to foreign countries even in the Single Market. Exports and cross-border sales are critical factors for increasing a country's competitiveness. According to Figure 18, 9% of EU firms engaged in sales in different European countries in 2019. The share of SMEs is at a similar level (8%), however, the respective share of medium enterprises is significantly higher (14%). Looking at the time trend during the period 2011-2019, it is evident that SMEs struggle to close the gap with medium-sized enterprises, and although the level of foreign sales has increased, also the difference between the shares of the two size categories has done so. These results corroborate the notion that expansion in foreign markets is a venture that is predominantly undertaken by the larger enterprises. SMEs were and still are in a rather disadvantageous position compared to their larger counterparts.

According to a briefing published by the European Parliament in March 2021,[13] large variances in the way the directive is implemented throughout the EU are present. Legal fragmentation across the Member States is a critical issue that hinders the optimal functioning of the Single Market. Legal barriers and regulatory burdens lead to high direct and opportunity costs, notably for SMEs, including innovative startups and scale-ups. Persisting legal uncertainty regarding applying national rules and conflicting court rulings are common obstacles that firms have to overcome for selling abroad. Common barriers to cross-border e-commerce include delivery and return issues, difficulties in complaint management, or restrictions on online sales established by commercial partners (Iacob and Simonelli, 2020). In addition, a particular issue that e-commerce is facing is the restrictions related to cross-border access to copyrighted content. Such barriers need to be addressed to tap into the full potential of e-commerce in the EU.

Figure 18: Enterprises with e-commerce sales to other EU countries



Source: European Commission

In October 2020, Oxera published a policy report regarding the impact of the DSA on business users building on a survey of 1,000 EU firms. The survey confirmed the assumption that firms could significantly increase their clientele and reach a wider customer base. Using the scale and scope of the efficiencies that platforms offer, combined with a consistent and clear business regulation that in the various Member States could unlock an additional €2.3 billion in revenue per year for the travel and tourism sector in the four countries surveyed (Bulgaria, Ireland, Germany and Spain). The

13 https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf#page=1&zoom=auto,-274,848

majority of respondents (71%) found the number of platform users key to their business's success, while 39% estimated that they would lose customers if platforms were to limit their users.

Iacob and Simonelli (2020) demonstrate the strategic importance of e-commerce and digital services for SMEs. They facilitate access to new markets and new consumer segments, boosting their growth and providing lower consumer prices (2% to 10% advantage over offline sales). Online markets improve the visibility of SMEs and limit upfront investments and operational costs, as well. The same study suggests that the effect of distance on trade can be up to 65% smaller for transactions online than transactions conducted offline.

Hence, it is not difficult to advocate for the potential benefits that SMEs could gain with such a harmonisation across Members States and the administrative burdens that could be mitigated. Here, the DSA package could enhance EU SME growth and ensure their sustainability, although the competition will be even tougher. However, the proposed regulation carries many challenges and risks that firms must confront. These issues could negatively affect business in the EU, creating a heavily regulated environment that strains economic activity instead of promoting it.

Firstly, a regulatory gap within the Single Market still exists since systemic legal issues are not appropriately addressed nor covered by the DSA-DMA package. National legal frameworks differ greatly on various elements regarding several crucial terms for the implementation of the package. The definition of illegal and harmful content certainly varies among Member States and, as well, law enforcement procedures are not harmonised. Although the DSA's initial approach establishes a more harmonised environment, the law system variations among the Member States creates a further burden for businesses and especially for SMEs. Moreover, illegal activities at the sector-specific level are tackled by specific legislative initiatives, but horizontally there is no instrument available (European Commission, 2020). Complementary to the other barriers found in the proposed DSA text, the definitions of several terms, such as the very large platforms, user, the good Samaritan clause, illegal content, need further clarification, as they seem to be rather vague concepts. It is not easy to develop a common framework but some clear definitions would help all stakeholders to have a common understanding of the elements that we are discussing.

The inclusion of harmful content could also have an additional negative impact since it increases the ambiguity of the legal framework. Regulating harmful content could violate the notion of democracy itself. The extent of the regulations and their implications could significantly distort the efficiency of the digital markets. The range, if any, regarding the interpretation of harmful terminology and the implementation by the Member States creates further ambiguity and uncertainty. The lack of explicit legal definitions that rely on interpretation is presently deterring firms, and particularly SMEs, from entering new markets and operating efficiently. This ambiguity acts as a disincentive for SMEs as they do not always have the legal resources to engage in time consuming disputes, either with competitors or customers.

A potential over-regulation of platform activities could lead to missed business opportunities. Flexibility is critical for businesses so they can tap into new opportunities that may otherwise not

come about. According to Oxera (2020), complicated sign-up procedures could discourage 28% of gig workers, while delays in job posts could hinder 40% of them from doing work at short notice. Furthermore, the same survey finds that increased platform liability or reporting requirements could limit ancillary features, such as reviews and AI applications, mitigating legal risks or avoiding administrative costs, hindering businesses' online activity. Changes to the regulatory environment could drive platforms to alter their services, risking a revenue loss for firms. Limited platform functionality (taken down content or increased fees) could cut revenues for 38% of businesses turning in a €1.4 billion per year loss in revenues for the travel and tourism sector in the four countries surveyed (Oxera, 2020).

The DSA's ex-ante regulatory regime could increase the regulatory burden as it does not replace the existing legal framework, and how it will interact with the national law and national authorities is not very well defined. Overlaps with this new instrument and its national equivalents exist. The efficient enforcement of ex-ante rules requires predictable parameters. Operators should be able to anticipate as much as possible whether they will be subject to the rules or not. For SMEs, in particular, it is more challenging to adapt to 27 different legal frameworks compared to one prominent player. Harmonisation and avoiding legal fragmentation are essential for SMEs, the backbone of the EU economy, and it must be guaranteed that they can take full advantage of the internal market. Therefore, it appears that the central coordination that the DSA aims to achieve would not necessarily lead to a more harmonised environment. Several pitfalls appear greatly complicating the operation in the EU Single Market.

The DSA's main elements include the special treatment of SMEs since they will have obligations proportionate to their ability and size. Large platforms might be able to tackle higher regulatory compliance costs easier compared to smaller players. Furthermore, the ability of new entrants to compete with large digital platforms is limited. According to the European Commission (2020), the impact of regulatory costs on online platforms is asymmetric and disproportionately affects small providers. It is argued that those costs are still comparatively modest for larger players even if they are greater in size. On the contrary, they can be unaffordable for startups and scale-ups wishing to develop in several Member States and operate in the Single Market.

At a first glance, the positive correlation between the firm's size and the responsibilities undertaken according to the new DSA framework could seem fair and easier to enforce. Still, illegal actions should be discouraged regardless of corporate size. What is illegal for large firms is also illegal for small firms and the resources available should not be used to tackle this issue. The intervention of the DSA in large platforms is on an important scale and will definitely affect their operations in the EU Single Market. Notably, the penalties for non-compliance with the new rules increase vastly as the platform's size increases. The EC's direct supervision is proposed for very large platforms, imposing fines of up to 6% of the global turnover of a service provider in the most serious cases and a temporary suspension of their services is also on the table.

The DSA includes "Know Your Customer" (KYC) obligations that will apply either to specific users or to a broader range of users. The extent of these protocols could significantly affect the operation of

the online markets. The additional identification could add an extra burden to platforms since more information and procedures would be required by registered users. Therefore, a potential declining rate of attracting new users emerges, hindering new and smaller players to a greater degree. As well, the lack of authority involvement in the consumer flagging procedure deserves further investigation since it could lead negative behaviour frustrating the optimal operation of firms. Taking into account the aforesaid, the final impact on SMEs needs further examination. The right balance must be found between the decreasing existing administrative burdens in doing business across Europe and imposing new invisible obstacles to SME potential growth.

4.1.1 Changes in competition in the Digital Single Market

It is also being discussed how the new legal framework can regulate digital competition. New crucial issues have emerged that traditional competition law has found it more and more difficult to deal with as the extent and the nature of competition has changed. Instead of a specific product-market, systems of complimentary services have emerged that attract both intermediate and end consumers. The frontier between digital and non-digital space has become blurred, and updating the legal framework now seems imperative. Platforms such as Airbnb or Uber are such examples. End consumers use the digital markets to receive services that do not stem from the online market. Even in the more traditional sectors such as the agri-food sector, it is evident that digitalisation and online selling is constantly increasing. For instance, new Agritech platforms which were previously considered merely as information points with a limited effect on the actual business model, are now turning into a key new element of the competition model.

In the digital area, instead of the existence of a product or market competition as traditional economic theory suggests, a new ecosystem competition is the current trend. Digital ecosystems result in efficient interaction among producers, content providers, developers, consumers, and other users, leading to value creation from (online or even offline) trade. Digital ecosystems can facilitate, for example, the production, distribution, marketing, sale or delivery of products and services by electronic means, the sale and/or shipment by traditional means of digital goods (products and services), as well as the transmission or storage of information as a service in its own right (Petropoulos, 2020). Competition can be developed among the different ecosystems (i.e., Apple versus Android smartphones) or inside the ecosystem itself when different firms offer substitute services/products within the same environment.

Considering the new structure of competition and the new dynamics it gives rise to, the DSA-DMA package could indeed enhance competition facilitating the entry of smaller firms. On the other hand, an intervention of this magnitude could lead to unintended consequences resulting in an impact quite different to that originally intended. The degree of intervention may not be the same in all markets or may diverge in the different sectors, bringing about unexpected negative consequences. As well, the objective of the DSA/DMA is to ensure competitive and fair markets in the digital sector. Still, the concept of “fairness” is a relatively new element to competition law and definitions are more than necessary.

In fact, the new regulation could actually deter fair competition instead of promoting it. The DMA gatekeepers can be defined following two different sets of criteria - quantitative criteria based on market figures and qualitative criteria, which are very broad. However, efficient enforcement of ex-ante rules requires predictable parameters. Operators should anticipate as much as possible whether or not they will be subject to the rules. Thus, uncertainty regarding potential penalties could be an important barrier for new entrants, particularly smaller firms that have neither the human resources nor the capacity to deal with them. The is a legal overlapping of this new instrument with its national equivalents, increasing the ambiguity. A new environment is created in combination with the rigid list of prohibitions that might deter or hinder developing firms from entry.

Over-regulation seems a credible hazard that could induce unforeseen spillovers. Combining a vague legal framework with the restrictive consequences for large platforms could lead to the big players over-reacting. Before the threat of severe penalties, large platforms could exaggerate their activities and limit the displayed content much less than the social optimum. Platforms and especially search engines do not provide only specific content to users, but they are also responsible for its prominence, a critical characteristic that seems to have been neglected. Interference of this size could lead not only to a significant distortion of competition, but also limitations in the exercising of fundamental rights.

4.1.2 The effect on competitiveness and innovation

An over-regulated market kills innovation as it greatly hinders any new efforts. The facilitation of doing business is a key factor for encouraging innovative activities, international research collaboration and technology developments. For example, platforms could use human oversight of every issue to avoid a penalty related to the zero-tolerance policy, preventing them from innovating with other technical solutions (such as AI tools).

Complying with regulatory and administrative requirements diverts too much energy from a growing business, particularly cross-border operations. The harmonisation that the DSA plans to achieve could incentivise innovative startups to stay and operate in Europe. However, if an over-regulated environment is the final result, EU-27 located startups might prefer to scale up in a different market, such as in the UK or the USA. Additionally, they could be acquired by the USA or by other funds, which means that the European economy would continue to lack in competitiveness. Thus, harmonising the rules offers an excellent opportunity for startups and scale-ups because critical market rules are clarified, as long as a level playing field is established against fragmented legislation.

Another critical issue of the proposed regulation is the positive relationship of regulatory costs and player size. New and medium-sized players may be deterred from developing their businesses because, in this case, their costs, in the case of a dispute, would rise considerably. Not only in terms of financial resources but also in human resources and knowledge.

Digital foreign direct investment and trade could also be discouraged since the new legal framework will add an undue cost to operating in Europe. The risk to invest in Europe would be much greater than in other markets. The uncertainty regarding potential severe penalties and the qualitative criteria that rely on vague definitions and rules could hinder foreign firms wishing to expand their services to the EU. A heavily regulated environment presents a substantial disadvantage for European international competitiveness, at the same time, when the contribution of digital trade to economic growth is becoming more important than ever.

Finally, the digital gap between the North and South of Europe should be taken into consideration. Traditionally, economies in the south rely more on the tourism sector for economic growth than the advancement of the technological or industrial sectors. Furthermore, SMEs, the main company type in the south, face resource shortages in the financial and human capital dimensions. Thus, investing in appropriate infrastructure and hiring ICT experts could be prohibitive for them. These facts could serve as a perspective on the differences in the digital readiness of the two parts of the continent. Harmonised legislation is vital for technological advancement and innovation growth but may not suffice considering the structural differences between these two areas of the EU. This gap must be bridged as soon as possible to establish inclusive and sustainable growth.

Conclusions

The digital market segments in the convergence era

Digital markets display high rates of dynamism and innovation, with products and services that have not only radically transformed entire economic and business sectors, but also spheres of human sociality and communications. Moreover, market dynamics have also shown an increasing rate of speed in the introduction and spreading of new services. We have witnessed sudden and radical shifts in the composition of market share, which continuously highlight the level of competitiveness digital platforms are exposed to, confirming a fair degree of scalability of many of these sectors. To quote some data, Instagram took six years from its launch to gain the same amount of monthly active users that TikTok managed to achieve in less than three years, while Facebook took more than four.

The relationship between innovation and competition is extremely complex, even more so in digital markets where new technologies risk becoming obsolete and outdated within a few years. Therefore, over-regulation could be harmful both in terms of technological development and competition on price, variety and efficiency.

From a more general point of view, various types of Internet sectors show a high degree of flexibility which makes the composition of market share vary according to different geographical macro-areas. In the case of e-commerce, for instance, new local-based large marketplace operators are emerging in Europe, Latin America and especially in Asia, where players like Amazon have not yetreached a 1% market share.

As for the segmentation identified by the DMA, it is worth noting that it is extremely complex to identify clear boundaries and distinctions, for instance, between video-sharing services like YouTube and social networks like TikTok. Indeed, there are now numerous cross-sector platforms, which are continuously seeking to expand their range of possibilities and services and aim at increasing user-friendliness and opportunities, as well as customising their services to meet new trends or consumer preferences.

The same can be said in relation to the advertising market, which has become very complex to analyse as different “channels” and formats are now not only converging, but also creating different subsectors in which players from different environments compete with each other for consumer attention. Converging technologies and strong competition for consumer attention has increasingly blurred the boundaries, so that, for instance, both the social media (such as Facebook and TikTok) and video sharing platforms (such as YouTube), as well as potentially personal communication tools such as WhatsApp, compete for video consumption on different formats and devices, making it extremely challenging to define the relevant markets.

This is also true for searches. Even if the global market structure is very concentrated, technological trends continuously challenge the incumbent, such as the spread of non-conventional search methods - voice search technologies, the use of social media platforms for commercial information searches, and the use of image recognition tools on mobile devices. The market is shifting from desktop to mobile services, making future developments harder to predict. The channels used are multiple, and involve searches, social media, banners, videos and other means in a mix that appears to be rather unclear at the moment.

Other market segments identified by the DMA are also impacted by geopolitical factors that, however, could have market implications, such as for operating systems (but something similar could occur, though with different dynamics and players, for cloud computing services). For instance, recent developments related to the Huawei ban in the United States pushed the Chinese company to develop its own operating system. If the HarmonyOS project, launched in 2019 by Huawei, reaches its target of including not only smartphones but also electrical appliances, creating a whole ecosystem of connected smart objects, it could undermine the well-established balance of recent years and lead to a further global reassessment in operating system market shares (and equilibria) over the next decade.

Today, very large online platforms which provide “open portals” play a key role in distributing and shaping information online. In some cases, they also assume responsibilities which seem to go far beyond the “pure” technological one (even if it falls shorter than typical editorial responsibilities). In these cases, platform design choices and security practices strongly affect user safety online, having the power to shape online content and discussions as well as the digital trade.

The dissemination of harmful content online and institution and main operator initiatives

As shown by the data provided by large platform operators, online threats are many, and are related to very sensitive topics (e.g., child protection) and are continuously growing. The platforms are at the forefront here and have adopted a number of strategies, mostly on a voluntary basis, in order to tackle these problems and support the EU institutions in combatting them. However, in the light of the available data, two kinds of considerations emerge. Firstly, the best practices implemented by the large operators show how trusted-flagger support is necessary, in particular, at the level of specific know-how. This is related to the trusted flaggers’ ability to draft general guidelines and also resolve the thorniest cases, where specific expertise or sensitivity is required. Secondly, given the constantly growing amount of illegal content posted by the users and analysed by the platforms, a human-machine collaboration appears essential to face these threats, also taking into account the value of the time factor. Indeed, not surprisingly, the same EU Code on countering hate speech online requires operators to act within 24 hours from it being reported. This is particularly true

considering the sensitivity of the issues involved, that include the protection of minors, as well as that of users from violent content such as hate speech and from terrorist organisations.

Thus, the strengthening of a coherent cooperation of large platforms, trusted flaggers and the most advanced algorithmic systems for a very fast and automatic content analysis and threat detection seems to have all the ingredients to ensure timely and fair intervention on large amounts of data. It would also take into account the number and sensitivity of those topics, which involve fundamental rights such as user (and minor) safeguarding, as well as the right to freedom of speech.
At the level of consumer protection, something similar can also be said for what concerns user protection from misleading online advertising and the online sale of counterfeit goods. Since many inexperienced users, especially during the pandemic, have recently turned to e-commerce, the number of bad actors willing to exploit the situation and conduct unfair practices or real scams has exponentially increased.

The main e-commerce platforms, also called on by the EU Commission to tackle these malpractices, use strategies involving a continuous monitoring of the advertising networks for compliance with their fair trade policies, using a combination of algorithmic and human reviews. Also in this case, data provided shows that platforms have found hundreds of thousands of illegal activities. On the other hand, almost 90% of interviewed consumers stated they would be happy for transactions to take longer to complete, if extra steps for authentication meant their information was better protected. The trade-off between a frictionless purchasing experience and the offer of a highly reliable protection system is not an easy one to manage. Even if facilitating consumer experience seems to be a primary need for merchants and e-commerce platforms, Signifyd's survey shows that about half of the consumers would tolerate no more than one negative experience with an online retailer before walking away for good.

Currently, the main e-commerce platforms adopt a series of security practices such as checking the identities of potential selling partners, applying codes that certify the unit's authenticity and involving automated processes using machine learning technology to identify bad actors. These strategies, in the most virtuous cases, have restricted the number of counterfeit good received by the final customers down to 0.01%. It is worth noting here that, to reach these targets, automated systems are essential and unavoidable. In the case of Amazon, for instance, data reveals that, for every single listing removed by a brand through the self-service counterfeit removal tool, automated protection removed more than 600 listings through scaled technology and machine learning.

In conclusion, in order to find the best tradeoff between consumer safeguarding and the protection of the rights related to the freedom of speech, a wise mix of automated and human intervention, also including support from authoritative sources, seems to be unavoidable.

The new digital regulatory framework

The DSA and DMA proposals will bring about important changes, redesigning the role and responsibilities of platforms and producing a strong impact on them and on the market.
Concerning the DSA proposal, even if the aim of ensuring an ecosystem capable of guaranteeing user rights is worthy of support, it should not be forgotten that, in the past, the lack of or a light regulation has favoured innovation and the rise of digital ecosystems that so far have provided huge benefits to society. Therefore, an **adequate balance is required** between the necessity to guarantee rights and freedom and the opportunity not to hinder, but rather to foster, innovation and competitiveness in the European Union through the introduction of an **over-regulated system**. To this end, in general, a **clear and certain regulatory framework** must be drawn up, ensuring coherence and avoiding duplication of the obligations stemming from the DSA and from other texts such as the Platform-to-Business Regulation and the Copyright Directive. In discussing the obligations placed on the platforms, **achievable and proportionate obligations** should be set, also considering the impact of **compliance costs** on small players and to avoid the risk that a regime too focused on large platforms may favour the displacement of illegal activities and content to smaller platforms, which are less equipped to deal with them.

Regarding the DMA proposal, the first point to be considered in the context of the legislative procedure, is the appropriateness of the choice of adopting an ***ex-ante*** **regulatory mechanism,** that is typical of more mature and less innovative markets. Even if this approach could potentially accelerate authority intervention and the collection of more data on possible anti-competitive conduct and ensure greater transparency and a deeper knowledge on the functioning of digital marketplaces, it may not be adaptable and flexible enough to manage the speed of technology and business chnages, thus, representing a real threat to innovation and competitiveness in Europe[14].

Moreover, if the principle that everything that is illegal offline should be illegal online seems sound (though with some limitations due to different technologies and contexts), the opposite should also hold true (for instance, for self-preferencing and advertising). However, the DMA (and partially the DSA) could create an artificial barrier not only between digital and physical ecosystems but also between digital and physical companies while the present and the future are moving towards convergence. Higher standards for digital intermediaries and platforms than for physical may slow down the digitalisation of traditional companies and, therefore, market contestability.

Another means to increase market contestability, creating greater innovation and efficiency gains, is by allowing gatekeepers to compete with each other (according to the moligopoly scenario[15]).

[14] For this reason, the paradigm shift from ex-post antitrust enforcement towards ex-ante regulatory compliance, implied by the DMA, has been called "precautionary antitrust" by some observers (Portuese A., *The Digital Markets Act: European Precautionary Antitrust*, ITIF, May 2021)
[15] Petit N. (2020), *Big Tech & the Digital Economy. The Moligopoly Scenario*, Oxford University Press.

Art. 5 and 6 in the DMA regulations would obstruct this possibility (that represents how innovation works in many instances, along with the other possibility of startups emerging against big players).

Concerning Ms. Schaldemose's Report, the following points need to be carefully addressed:

1) limiting the liability exemption where it is assessed that an online platform has control/authority/influence over the trader could negatively affect the possibility for many SMEs to trade their products on new markets, raising their costs or eliminating them;

2) in order to improve consumer awareness of commercial content, the Report suggests to have prominent and harmonised markings of advertisement. While the intent may be right, it seems to undervalue the role of different technologies and their evolution, technically making the proposal either cumbersome or not at all feasible;

3) the Report proposes that any recommender system should, by default, not be based on profiling, and that consumers subject to recommender systems using profiling should be able to view and delete any profiles used to curate the content they see. While the latter measure could provide important benefits for consumers, the former may greatly reduce the positive impact on consumers of modern technologies such as Artificial Intelligence;

4) a "must-carry" obligation to ensure that information of public interest is high-ranked in the platforms algorithms may infringe on the freedom of expression and free market principles unless it is limited to exceptional situations;

5) the Report finds that greater accountability on algorithms should be introduced in the proposal, enabling the Commission to assess the algorithms used by very large online platforms and determine whether they comply with a number of requirements, providing for sanctions in the case of infringement. This measure appears to be clearly disproportionate and may seriously interfere with business models and technology developments, heavily hindering innovation.

6) leaving the decision to suspend social media accounts covering matters of public interest, including those of politicians, to the relevant judicial authority instead of to the respective platform, after a due process (with appeal procedures), appears intrusive and dangerous, paving the way to a regime of state control that in some countries could result in a serious breach of democratic principles.

As for Mr. Schwab's Report and the non-paper released by the governments of France, Germany and the Netherlands, it should be noted that:

1) a further reduction in scope to fewer gatekeepers risks putting the brake on the moligopoly contest that is an important source of competition in digital markets. As such, it should be overseen by the competent authorities but not ruled out or over-regulated;

2) the tightening of merger controls could seriously impact the exit strategy of many startups, including many Europeans, limiting their development;

3) ruling out commitments from the menu choice reduces the flexibility that uncertainty in fast changing markets seems to require, instead of leaving to the burden of possibly decisive calls to litigation, a sort of bomb (for all parties), but without defusing it;

4) shorter timeframes and closer deadlines could lead to quicker but also unfair and rushed judgements (taking into account the exceptionality of the mechanism);

5) while pooling national resources and fostering stricter coordination and cooperation among Member States to support the Commission appear perfectly sound, fragmentation based on national rules and enforcement should be avoided, leaving the steering to the EU.

Economics effects from the DSA package

The introduction of the Digital Services Act package will affect the economic and entrepreneurial landscape of the EU in multiple dimensions. The reconstruction and updating of the current regulation and the introduction of novel directives to cover emerging aspects previously disregarded are imminent. On the other hand, regulatory intervention should be designed cautiously as over-regulation in digital markets is bound to have counter-effects and affect market functionality. Considering the digital market trends and the changes that the pandemic has caused, the emergence of digital markets offers fertile ground for new business ventures and the improvement and expansion of already established actors. SMEs make up approximately 99% of all EU enterprises, and current statistics indicate that firm size is closely correlated to success in digital markets. Thus, fostering the Digital Single Market could lead to a wave of positive spillovers.

Nevertheless, the proposed regulation gives rise to many challenges and risks that firms have to confront. These issues could negatively affect EU business, creating a heavily regulated environment that strains economic activity instead of promoting it. The differences in the legal frameworks among Member States concerning various crucial elements for the DSA implementation could create a further burden for businesses, and especially for SMEs. The definitions in the regulation (such as the very large platforms, users, the good Samaritan clause, illegal content) need further clarification, and the inclusion of harmful content could have an additional negative impact. The extent of the regulations and their implications could significantly distort the efficacy of the digital markets. Efficient enforcement of ex-ante rules requires predictable parameters. Operators should

be able to anticipate as much as possible whether they will be subject to the rules. Uncertainty acts as a disincentive for SMEs to thrive due to their limited resources.

Utilising the DSA-DMA package to respond to the updated structure of competition could indeed enhance competition facilitating the entry of smaller firms into the market. On the other hand, an intervention of this magnitude could also result in an impact different to the one originally intended. The degree of intervention may not be the same in all markets or may diverge amongst the different sectors, bringing about unexpected adverse effects. As well, the objective of the DSA/DMA is to ensure competitive and fair markets in the digital sector. However, the concept of "fairness" is still a relatively new element to competition law, and definitions are more than necessary. The qualitative criteria for being an important gateway are very broad, while efficient enforcement of ex-ante rules requires predictable parameters. Ambiguity regarding potential penalties could be a big barrier for new entrants, particularly for smaller firms that have neither the human resources nor the capacity to deal with them. Under the threat of severe penalties, large platforms could exaggerate their activities and limit the displayed content to a much lesser degree than the social optimum.

An over-regulated market kills innovative activities since it greatly hinders any new efforts. The facilitation of doing business is a key factor for encouraging innovative activities, international research collaboration and technology development. Complying with regulatory and administrative requirements diverts too much energy away from a growing business, particularly cross-border operations. If an over-regulated environment is finally formulated, EU-27 located startups may prefer to scale up in a different market such as in the UK or the USA. Additionally, they could be acquired from abroad, which means that the European economy will continue to fall behind in competitiveness.

Digital foreign direct investment and trade could also be discouraged since the new legal framework will add an undue cost to operating in Europe. A heavily regulated environment is a disadvantage for European international competitiveness, while the contribution of digital trade to economic growth is becoming more important than ever. Finally, the digital gap between the North and South of Europe should be taken into consideration. The EU must bridge this gap as soon as possible as common legislation is vital for technological advancement and innovation growth.

Bibliography

Accenture (2020), *Hyperscale your cloud journey: Partner for more value*.

Amazon (2021), *Brand Protection Report*.

Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T. and Van Alstyne (2021), M., *The EU Digital Markets Act, Publications Office of the European Union*, Luxembourg, ISBN 978-92-76-29788-8, doi:10.2760/139337, JRC122910.

Calvano, E., & Polo, M. (2021), "Market power, competition and innovation in digital markets: A survey". *Information Economics and Policy*, *54*, 100853.

Crane D., (2020), *Ecosystem Competition*, available at https://one.oecd.org/document/DAF/COMP/WD(2020)67/en/pdf

Ecommerce Foundation (2019), *European E-commerce Report*.

Ezrachi, A., & Stubb, M. (2018), *Digitalisation and its impact on innovation.*

European Commission (2020), *5th evaluation of the Code of Conduct*.

European Commission (2020), COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

European Commission (2021), *Disinformation: A threat to democracy*

European Commission (2021), *Science, Research and Innovation Performance of the EU 2020 "A fair, green and digital Europe"*

Facebook (2019), *Report on the implementation of the Code of Practice for Disinformation*

Facebook (2021), *Transparency reports*

Fletcher, A. (2020), *Digital competition policy: Are ecosystems different?*, available at https://one.oecd.org/document/DAF/COMP/WD(2020)96/en/pdf

Google (2019), *Annual report "EC EU Code of Practice on Disinformation"*

Iacob, N., Simonelli, F. (2020), *How to Fully Reap the Benefits of the Internal Market for E-Commerce?*, study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

IDC (2020), *European Data Market Monitoring Tool*

IDC (2021), *Smartphone market share*

Kepios (2021), *Global overview report*

Marqueta (2020), *Why consumers don't understand card fraud… and what payments innovators have to do about it*, 2020 Fraud Report.

Microsoft (2019), *Self-assessment and report on compliance with the EU code of practice on disinformation*

National Institute of Standards and Technology (2011), *The NIST Definition of Cloud Computing*

Negru S., Rodriguez R. A. (2021), *Frauds in the Ecommerce space: trends to watch in 2021*

OXERA (2020), *The impact of the Digital Services Act on business users*, Policy report prepared for Allied for Start-ups

Petit N. (2020), *Big Tech & the Digital Economy. The Moligopoly Scenario*, Oxford University Press

Petropoulos G. (2020), *Competition Economics of Digital Ecosystems*, available at https://one.oecd.org/document/DAF/COMP/WD(2020)91/en/pdf

Portuese A. (2021), *The Digital Markets Act: European Precautionary Antitrust*, ITIF

Statcounter global stats (2021), *Browser Market Share Worldwide*

Statista (2021), *Digital Market Outlook*

The Global Web Index (2021), *Social media marketing trends*

The Global Web Index (2020), *Survey Data on International Consumer Behaviour*

The Paypers (2020), *Fraud Prevention in Ecommerce, Report 2020/2021*

Twitter (2019), *Progress Report: Code of practice against disinformation*

Twitter (2021), *Transparency Reports*