icom
institute for competitiveness

EU'S PATH TO COMPETITIVENESS

HOW DIGITAL, ENERGY AND HEALTH CAN LEAD THE WAY FORWARD

REPORT DEC 2021

icom
institute for competitiveness

EU'S PATH TO COMPETITIVENESS

HOW DIGITAL, ENERGY AND HEALTH CAN LEAD THE WAY FORWARD

DECEMBER 2021

AUTHORS

Silvia Compagnucci

Stefano da Empoli

Maria Rosaria Della Porta

Maria Vittoria Di Sangro

Afroditi Karidomatis

Michele Masulli

Eleonora Mazzoni

Thomas Osborn

Domenico Salerno

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CHAPTER 1 describes the most important trends in the digital sector and the evolution of the European regulatory framework on online platforms, data, 5G, AI and cybersecurity. **Paragraph 1.1** focuses on the role of the **digital platforms in the market and the Digital Markets Act (DMA) proposal**. The growing importance of the digital market can be seen as one of the most significant changes of our era, as it is an enabling element for economic growth and a driving force for the transformation of daily activities. In recent years, e-commerce has boosted both sales and turnover, becoming a key element for global retail trade. In 2020, the volume of sales generated globally from online purchases amounted to $2.855 billion, while estimates attest to a total turnover growth of 47%, to reach $4.200 billion in 2025. A fundamental role in the impressive growth of the sector is played by the large digital marketplaces. These platforms have reached a global dimension and are used by a huge mass of consumers.

A branch of the digital market that has become particularly important in recent years is the **mobile sector**. Based on some estimates made in January 2021 on a panel of Android users, the time spent on mobile devices exceeds an average of 4 hours a day, 44% of which is dedicated to sharing content, communication and social media, while 26% to entertainment and video apps and 9% to video game apps. By observing the data released by Airnow on the most downloaded apps from Apple and Android stores in the world in October 2021, it is possible to see how among the apps with the highest number of users there are all those that refer to social media. The apps of the Facebook group (Facebook, WhatsApp, Instagram, Messenger) are the most downloaded (75.42M), but also those of other social networks such as TikTok (27.44), Telegram (26.3) and Snapchat (21.1) record excellent performances.

As regards the **social network sector**, it can be observed that it actually includes a wide range of services that sometimes have quite different characteristics. While most of these allow users to connect, communicate and share content of a different nature (texts, images, videos and even direct streaming), they differ in other aspects, such as the type and scope of the exchange, public or private (both text, voice or audio-visual) in real time, and the ability to create groups and communities online. Still others offer more specific services, for example by focusing on particular aspects (e.g., publishing and sharing images and / or videos). Consequently, the definition of these platforms tends to transcend the boundaries of such categories, complicating the analysis, making it difficult to provide a clear and comprehensive picture of the sector and its sub-categories. To regulate the new critical issues connected to the affirmation of large online intermediaries and platforms, on 15 December 2020, the European Commission submitted the **Digital Markets Act (DMA),** one of the most important milestones of the

EU digital strategy. The proposal, which is triggering an enormous debate among stakeholders and numerous requests for change, defines the prerequisites for qualifying a provider as a gatekeeper, sets several obligations and prohibitions on gatekeepers and attributes the Commission very important powers 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.

Paragraph 1.2 also focuses on the new regulatory framework on platforms and, specifically, on the **Digital Services Act (DSA) proposal**. The DSA amends, while maintaining its key principles, the E-commerce Directive (Directive 2000/31/EC) ensuring the best conditions for the provision of innovative digital services in the Internal market, contributing to online safety and the protection of fundamental rights (above all, freedom of expression and information) and establishing a sound and sustainable governance model for the supervision of intermediary service providers. Specifically, the proposal is a **horizontal instrument** to create a safer and trusted online environment putting in place a framework of **layered responsibilities targeted at different types of services** (i.e., intermediary, hosting, online platform, and very large online platform services) and proposing a set of **harmonised EU-wide asymmetric obligations** to guarantee transparency, accountability and regulatory overseeing of the EU online space. The same proposal places **specific obligations on the MSs** 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.

The debate over the DSA takes place in the context of a **growing e-commerce market**. The volume of activities and revenues linked to online shopping has been growing for years, but the pandemic has drastically accelerated this. Eurostat data shows that the percentage of individuals that bought online at least one good or service within the last three months rose in the EU-27 from 27% in 2010 to 49% in 2019, recording a 5 percentage point jump in 2020, up to 54%.

One of the main issues linked to the thriving e-commerce concerns the increase in **bad actors and fraudsters on the web**.

The spread of **social networks** is 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. According to the results of the survey conducted by Eurobarometer for the EU Commission, out of over 30,000 Internet users in all MSs, 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.

Another major market that is developing on the web is **advertising.** Differently from the traditional advertising market, the digital one has experienced a continuous growth during the last 15 years with an average annual growth of about +20%, with display ad spending on the rise. While traditional display ad registered a -1.6% decrease in 2020, display ad spending using programmatic saw a 7.6% increase.

Paragraph 1.3 describes the trends of data economy and enabling technologies in the EU and the evolution of data regulation. Nowadays, most economic activity depends on the sharing of and the use of data and, in the future, this trend will continue to increase with a huge economic impact. In 2020, **the value of the data economy** exceeded the threshold of €300 billion for the EU-27 and, in relative terms, the impact of the data economy on the EU-27 GDP is 2.8%, up by 0.8 percentage points compared to 2015.

Considering that the digital revolution finds its lifeblood in data, the attention of European institutions has for years been on two different aspects – the protection of personal data and the creation of an ecosystem enabling data circulation and use.

In February 2020, the Communication "***A European Strategy for Data***" outlined the European strategy, to make the EU the most attractive, secure and dynamic data-agile economy in the world – empowering Europe with data to improve decisions and better the lives of all of its citizens. The strategy is focused on four pillars and several key actions to encourage a cross-sectoral governance framework for data access and use, to strengthen Europe's capabilities and infrastructures for hosting, processing and using data, interoperability to reinforce competences and skills and to create common European data spaces in strategic sectors and domains of public interest (specifically, manufacturing, the Green Deal, mobility, health, finance, energy, agriculture, public administrations and skills).

In this context, the Commission will foster synergies between the work on a European cloud federation and MS initiatives, such as the "Gaia-X" cloud project, a federated data infrastructure to enable the management, access and control of data belonging to EU citizens and businesses. In addition to the commitment to creating the European federal cloud within the framework of the Gaia X project, on December 2020, the European Commission launched a **European Alliance on Industrial Data, Edge and Cloud**, made up of representatives from MSs, cloud computing providers and industrial cloud users.

Implementing the strategy for data, on 25 November 2020, the Commission proposed a regulation on European data governance (**Data Governance Act**) which aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU.

More dedicated proposals on data spaces are expected to follow in 2022, complemented by a **Data Act** to foster data sharing among businesses, and between business and governments.

Paragraph 1.4 analyses the main trends of the AI market

and describes the European approach and initiatives on AI. The growing interest by companies in these new technologies is confirmed by the exponential growth registered by the **AI market** in recent years. According to the latest release of the IDC (International Data Corporation), **worldwide revenues for the AI market**, including software, hardware, and services, is estimated to grow 15.2% year over year in 2021 to $341.8 billion. The market is forecasted to accelerate further in 2022 with a 18.8% growth and remain on track to break the $500 billion mark by 2024. Interest in ai is also very strong in Europe. The **European AI software market** is expected to experience significant growth in the coming years, with revenues increasing from around US $2.09 billion in 2018 to an expected 26.5 billion by 2025.

However, comparing the EU to China and the US, a pattern of a clear competitive disadvantage seems to emerge. The gap in the overall amount of investments appears to be the main reason for Europe lagging behind. Moreover, the US and China account for most **AI start-up** investments (80%), and they were followed by the EU-27 representing almost 5% of the value of VC investments in AI start-ups.

The EU disadvantage seems to emerge also in terms of **AI publications and patents**, especially compared to the US.

An analysis of single EU states reveals substantial differences, with some countries able to keep pace even at the international level and others not very inclined to full AI adoption.

In order to give an idea of the degree of AI development in European countries, **I-Com has developed a new synthetic index on AI development in the European countries** that takes into account some variables relating to the industrial and research AI ecosystem in the various MSs, as well as the level of the adoption of some AI technologies.

Ireland tops the rankings with a score of 100, followed by Malta and Finland with scores of 95 and 78, respectively. These countries, despite being small in terms of size compared to others, have a good AI ecosystem. For instance, Ireland is emerging as a leading player with 273 AI firms, many having filed patent applications. Moreover, Ireland has a much higher percentage than the EU average (2%) of enterprises that analyse big data internally using machine learning (20%). At the bottom of the ranking, we find the countries of Eastern Europe, where both the industrial and research AI ecosystem sees a lower number of active AI players or where the level of adoption of technologies is very low.

Despite the many benefits, the use of AI technology also presents some concerns, especially with regards to human rights and possible threats to people's safety. One of the major causes of these concerns can be traced back to the lack of a well-defined regulatory framework that can set clear principles for its development and use. Following the **White Paper (Artificial Intelligence: a European Approach to excellence and trust), published in February 2020,** in April 2021, the European Commission presented the **"AI Package"**, which consists of three documents – a Communication on Fostering a European Approach to Artificial Intelligence, the 2021 update to the

Coordinated Plan with Member States, and a proposal for an AI Regulation laying down harmonised rules for the EU (Artificial Intelligence Act). The core element of this package is, of course, the proposal of an **Artificial Intelligence Act**, which has been described as "the first ever legal framework on AI". The AI Act aims to create an environment of trust among European citizens in AI, by imposing specific obligations on actors. More specifically, following a risk-based approach the AI ACT establishes a list of prohibited practices for all AI systems and differentiates between AI that creates: (i) unacceptable risk; (ii) high risk; and (iii) low or minimal risk.

Paragraph 1.5 is focused on 5G networks. Throughout 2021, Europe has made a number of important steps towards the development of 5G networks. Significant improvements have been made in the allocation of a large number of frequencies through national auctions, and in the launch of innovative services by a large number of operators. However, the EU-27 average percentage of **assigned spectrum** is only 45.8%, as a number of countries still present impacting delays. On the other hand, the **adoption of 5G** is accelerating worldwide, and about 8% of all connections are already being made on 5G. Indeed, according to GSMA's estimation, in 2025, Asian countries will reach more than a billion connections on 5G networks (more than 800 million in China and more than 160 million in the Pacific-Asian countries), compared to about 240 million connections in Europe and 220 million in the US. In proportional terms, the percentage of 5G usage is expected to be significantly lower in Europe (about 35% of total mobile users) than in the US and Asia (up to over 50% of users). Wide availability of high-performance networks is a prerequisite for citizens, businesses and public administrations to fully enjoy the benefits of digitalisation. The EU institutions, aware that the EU is lagging behind other parts of the world, have set increasingly challenging connectivity targets and taken action in a range of areas to improve connectivity and define harmonised rules for connectivity services. From the adoption of the Digital Agenda for Europe in 2010, several initiatives have been set and ambitious goals have been fixed.

On 9 March 2021, the European Commission published the Communication ***"2030 Digital Compass: the European way for the Digital Decade"*** that has underlined the importance to ensure an excellent and secure connectivity for everybody and everywhere in Europe and achieve gigabite connectivity by 2030. To this end, any technology mix can be used even if the focus should be on the more sustainable next generation fixed, mobile and satellite connectivity, with very high-capacity networks including 5G being rolled out.

After the adoption of the **2018 European Electronic Communications Code** updating the rules for radio spectrum management across the EU, and calling for creating a stable and harmonised regulatory environment and facilitating innovation, particularly through 5G networks, to accelerate infrastructure development, in September 2020, the Commission adopted **Recommendation n. 2020/1307 on a common Union toolbox. This aims to reduce the cost of deploying very high capacity networks and ensure**

timely and investment-friendly access to 5G radio spectrum, and to foster connectivity in support of economic recovery from the Covid-19 crisis.

In July 2020, the European Council agreed on the **Recovery and Resilience Facility**, the centrepiece of NextGenerationEU, a temporary recovery instrument that allows the Commission to raise funds to help repair the immediate economic and social damage brought about by the pandemic. In order to receive funds from the Facility, MSs must prepare national recovery and resilience plans of which at least 20% must be allocated in support of digital transformation. Among flagships areas for investments and reforms, the roll-out of rapid broadband services is one of the most important.

In October 2020, the **Connectivity Special Group**, made up MS representatives responsible for the area of electronic communications and the Commission, was established to assist the states in identifying and agreeing on the best practices and, upon request, in the implementation and reporting of the toolbox.

In line with the roadmap set out in the recommendation, Member States, in close cooperation with the Commission, agreed, on 25 March 2021, on a **Connectivity Toolbox** outlining a set of best practices to reduce these costs, promote access to physical infrastructure and streamline authorisation procedures for civil works.

Paragraph 1.6, finally, analyses the critical issues connected to **cybersecurity**. In fact, together with many advantages (always accessible, everywhere and at any moment), this relatively new way of living has brought to light many new problems in terms of security and, specifically, cybersecurity. The dimensions that this problem has assumed are even more evident by observing Europol data. In 2019, the agency focused 20.1% of its total operations on the fight against cybercrime. According to a study carried out by Comparitech in the third quarter of 2019, 9.68% of computers and 3.04% of mobile devices in the EU were infected with **malware**. Comparing the European data with those of the other major world economies, we can see how the EU ranks first for the percentage of infected computers, ahead of China, Japan, the USA, South Korea and the UK. Instead, where mobile devices are concerned, the EU states are, on average, more protected than those of all the other geographical areas considered except for Japan.

From the point of view of **organisations**, suffering a cyberattack that involves the loss of data results in a highly damaging negative impact both from the economic point of view and the loss of trust on the part of users. According to an IBM study, the average **cost of violations** globally is estimated to be around $4.2 million in 2021. By observing the time trend, it is possible to see how the economic repercussions on companies affected by cyberattacks have grown by 15% between 2017 (the year in which they amounted to $3.62 million) and 2021, of which, by 9% only in the last year.

Since 2013, the EU has worked on a wide legislation on cybersecurity to appropriately face the challenges of digitalisation. The EU Cybersecurity Strategy of 2013 was adopted to safeguard the online environment providing security and freedom. It outlines the EU's vision and proposes actions aimed at pursuing cyber

resilience, reducing cybercrime, developing an EU Cyber Defence Policy and fostering the industrial and technological resources required to benefit from the Digital Single Market.

Nevertheless, an important step forward in the EU legislation on cybersecurity was the **Directive on Security of Network and Information System** (the **NIS Directive**), adopted by the European Parliament on **6 July 2016**, entering into force in August 2016.

With **Regulation 2019/881**, known as the **Cybersecurity Act**, the EU reached a political agreement to strengthen the EU Agency for Cybersecurity (**ENISA**) and established a wide certification framework on digital products, services and processes.

On **16 December 2020**, the Commission launched several initiatives on security. Specifically, the Commission adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive), a proposal for a Directive on the Resilience of Critical Entities (2020/0365 COD) and the new Cybersecurity Strategy. Starting from the consideration that transport, energy, health, telecommunications, finance, security, democratic processes, space and defence are heavily reliant on networks, information systems have become increasingly interconnected and these cross-sector interdependences have increased vulnerabilities to cyberattacks, the Commission has launched a strategy focused on three pillars and connected initiatives. Here, the setting up of the **European Cybersecurity Competence Centre (ECCC)** in Bucharest is crucial. Its goal is to bring together various organisations from industry, academia and civil society to create a so-called cybersecurity skills community and collaborate with a network of national coordination centres.

CHAPTER TWO analyses the main facts that have occurred during the last two years in the EU as a result of the spreading of the Covid-19 pandemic. The **health emergency** has created an **unprecedented burden on the European Member States**, leading to the European institutions having to rapidly intervene to address the main bottlenecks and **strengthen the European capacity to respond to common threats**. Twenty months on from the outbreak of Covid-19 in Europe, the importance of a strong and cohesive EU especially in relation to public health is still a central matter to be addressed.

Paragraph 2.1 analyses **the first responses of the MSs and the EU in the early months of the pandemic,** with a view to better understanding the role that the EU should have in such extraordinary (but not unrepeatable) circumstances.

When the initial spread of the virus rapidly escalated, **the EU struggled to play a coordinating role**, complementing national policies to help countries in facing common challenges, such as a lack of sufficient healthcare organisation and provision, so that each state was better prepared for the healthcare challenges.

The pandemic has clearly shown that the EU needs a crisis-resilient system and the means to produce medicines within the EU to ensure timely access to essential medicines for citizens and hospitals under

all circumstances. A key political lesson of this crisis is that **further collaboration is required in Europe to face public health challenges** such as the one we are still living, and the EU seems to have learnt the lesson. That is why on September 2021, **the EU established the European Health Emergency Preparedness and Response Authority (HERA)**. The establishment of a European biomedical advanced research agency allows not only for overcoming the fragmentation of the expertise currently scattered amongst various European bodies and organisations, but also plays the role of coordinating the research of diagnostic and therapeutic solutions with the aim of being prepared for the management of epidemic and pandemic emergencies, unfortunately expected to reoccur over time. The creation of such an agency also strengthens the role of the ECDC whose mandate is to work with national and EU-level health authorities to facilitate cooperation, and to provide the evidence base needed for effective action. **Paragraph 2.2** describes the aftermath of the early months of the pandemic which led the EU onto the **road to the creation of the European Health Union.**

The pandemic put an immense strain on European countries, testing the resilience of every country's health and economic systems, together with the ability of the European Commission to develop a coordinated set of responses to what is still a common threat. The **lack of investment in health systems,** while saving money in the short term, can have devastating effects on a economy and society in the long term. Moreover, it has highlighted that other health emergencies will occur in the future, especially concerning the increasing burden of non-communicable diseases which will require placing the patient at the centre of health policies and the uptake of new innovations in treatment.

The European Commission is committed to building a strong **European Health Union**, where all EU countries prepare and respond together to health crises, with available, affordable and innovative medical supplies, and where countries work together to improve prevention, treatment and aftercare for diseases such as cancer. **The key initiatives to build a European Health Union include a Pharmaceutical Strategy for Europe, crisis preparedness and response measures and the European Plan to Beat Cancer.**

The pandemic has clearly demonstrated the need to revise how the Union supplies medicines to its population, as well as highlighting the importance of establishing the conditions and means to produce medicines within the EU, guaranteeing accessibility, sustainability and safety. **Returning the production of pharmaceutical raw materials to Europe is one of the cornerstones of this strategy, as is the need to increase innovation in the areas of unmet needs.** Indeed, although Europe has a strong manufacturing footprint, the supply chain still relies heavily on subcontractors to produce pharmaceutical raw materials outside the EU – in fact, between 60% and 80% of the active chemical ingredients are produced outside Europe, mainly in China and India. On 1 June 2020, the European Commission began working on this problem, publishing a roadmap for drawing up a European Pharmaceutical Strategy

and launching a public consultation. The aim was to promote competitiveness, the ability to innovate and the sustainability of the EU pharmaceutical industry. Then, **on 25 November 2020, the Commission published the final document of the Pharmaceutical Strategy for Europe**[1], in line with the new Industrial Strategy for Europe and the priorities outlined in the European Green Deal, with the European Cancer Plan and the European Digital Strategy.

Bringing the production of pharmaceutical raw materials back to Europe is a cornerstone of this strategy, requiring the design of an adequate industrial policy, and the creation and preservation of incentives. The latter obviously also depends on, but not only, the definition of the price negotiation by MSs.

The medium/long term objective is, instead, to overcome **the fragmentation of the health ecosystem also from an industrial point of view.**

While working on the industrial side, the EU also needs to increase capacity building, and the digital upskilling of employers working in the health sector, while also intervening to leverage the health data potential, which is still underdeveloped and underused. **That is why one of the corollary initiatives of the pharmaceutical strategy is the European Health Data Space and Eu4health**. The ambition is to prepare a reform for the pharma strategy packet by the end of 2022. The EU understood that industries need to partner up with institutions for better collaboration, and to avoid shortages and increase production capacity. This is why EMA is the second EU agency whose role and operation needed to be reinforced. The Parliament and the Council reached an agreement at the end of October 2021 to **strengthen the EMA's role to avoid potential future shortages of medicines and medical devices**. Here, it is crucial to have **monitoring and reporting procedures, and to develop IT tools to check on supply chains in order to prevent major crises from escalating**. Moreover, the European Commission proceeded with a **Proposal for a Regulation on Serious Cross-border Health Threats,** in order to create a more robust mandate for coordination at EU-level. The regulation applies to threats of biological origin (communicable diseases, antimicrobial resistance and biotoxins), threats of chemical origin, threats of environmental and unknown origin, and events which may constitute public health emergencies of international concern under the International Health Regulations (IHR), provided that they fall under one of the previously listed categories.

The main operative consequences would be the **creation of an EU health crisis and pandemic preparedness plan**, complemented by national plans and transparent reporting of capacities, strengthened and integrated surveillance systems, enhanced risk assessment for health threats, increased power to enforce a coordinated response at EU level through the Health Security Committee, and an improved mechanism for recognition of and response to public health emergencies.

Lastly, the EU adopted the **Europe Beating Cancer Plan** on February 2021. Since cancer is the second leading

1 https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020DC0761&from=EN

cause of mortality in EU countries after cardiovascular diseases, accounting for 29% of all deaths among males and 23% among females across all EU MSs, improving prevention and care is crucial. The actions and flagship initiatives included in the plan cover and tackle the entire pathway of the disease – prevention, diagnosis, treatment and the quality of life of patients and survivors. It will enable expertise and resources to be shared across the EU supporting countries, regions and cities with less knowledge and capabilities. It will also help researchers to exchange findings in the EU and access health data on the potential causes of cancer and its promising treatments. As much as 30% of the world's stored data is currently produced by health systems, but the health sector lags behind in exploiting this potential and making information out of data. The **European Health Data Space (EHDS)** will enable cancer patients (and not only) to securely access and share their health data in an integrated format in the electronic health records between healthcare providers and across borders in the EU. The Commission will pursue work with MSs on a common exchange format for electronic health records and to tackle data security, privacy and interoperability.

In **Paragraph 2.3, we analyse how the emergence of new technologies and enhanced connectivity have spurred the exponential growth of health data and how the European Health Data Space fits the EU purpose of leading the forthcoming data-driven society**. Nowadays, a vast quantity of this remains hidden in private or proprietary and project specific registries. Nevertheless, the promotion of health-data exchange is highly important in supporting all kinds of clinical research, guaranteeing new treatments, medicines, medical devices and health outcomes and to enhance the responsiveness of the whole system. However, there are challenges such as limitations and obstacles created by interoperability and the differing legal regimes within the EU that govern the access and right to process health data for research purposes, a lack of high-quality data, organisational and structural barriers and the need for a highly ethical approach essential to build trust with individuals and strives to use the data for the greater good. Having access to a growing volume of data and being able to process it are both key to growth and innovation. Data-driven innovation can deliver important benefits for citizens and for the European economy, from refining decision-making to improving public services.

The European Data Strategy aims to make EU a leader in a data-driven society. Here, it is essential to be aware that governing health data for its secondary use is a distinct case in EU data governance. **Governing health data requires a specific mechanism and cannot be governed by horizontal legislation alone, such as the proposed Data Governance Act**. There are many different reasons why health data needs *ad hoc* initiatives. First of all, the **respect of a patient's right to protect personal data**. With the General Data Protection Regulation[2] (GDPR), the EU has underlined the protection of personal health data as a fundamental

2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434

right. Yet, aggregated health information consists of personal health data, where it is essentially the basic input for research and policy-making. At the same time, health data is special in that it regards a subject with high societal saliency – that is, public health. The sharing of health data and the implied benefits for the wider public, could be the grounds on which the rights of an individual or patient may not prevail. This is clear in the case of infectious diseases, as well as societal or environmental health threats where the use of data is of vital and urgent interest, but also when developing prevention or treatment of other diseases. Moreover, a responsible secondary use of health data is imperative to maintaining **citizen trust and significant investments in data processing**. The growing volume of health data and increasing variety of methods to use it for secondary purposes is a growing source for the development of new businesses and innovation in personal health, health services, health care management, development of effectivity and quality of health services. The GDPR allows for the use of data in the private sector for research purposes. However, national health systems vary in Europe – from publicly funded systems, to semi-public health insurance and provision of health services, to totally private systems. The Data Governance Act separates governance mechanisms and rules for data from public or private sectors, but it does not specifically differentiate between health data provided by the public or private sectors. To date, many EU states have already established a national health data governance framework, or are in the process of establishing one. Far fewer states, however, have embedded these nationwide and centralised regulatory frameworks for the access and reuse of health data in national law. As well, several MSs have reported experiencing data governance challenges to developing health data infrastructures, with most mentioning legal or policy barriers to public authorities undertaking data linkages and sharing data among public health authorities. This could lead to fragmentation and hamper the unambiguous access and exchange of health data, which, in turn, proves the need for a more unified regulatory framework.

The creation of a **European Health Data Space** is one of the key priorities of this Commission in the area of health. The main purpose of the EHDS is to promote health-data exchange and support research on new preventive strategies, as well as on treatments, medicines, medical devices and outcomes. As a policy initiative, the EHDS aims to provide a common framework across EU Member States for the sharing and exchange of quality health data such as electronic health records, patient registries and genomic data.

However, the EHDS should not only be limited to the promotion of cross-border services or data transfers. It should also address the broader issue of data access for permissible data use subject to appropriate safeguards, e.g., for research and innovation purposes, and not solely for the provision of care.

CHAPTER 3 discusses the role of the EU in global decarbonisation. Specifically, **Paragraph 3.1** deals with ambitious **European energy transition policies**.

Global energy demand reached **13,297 Mtoe in 2020**, a **10% increase compared to 2010**. The **EUn** is also the only region with the largest **share of renewables in the energy mix** with **13% in 2020**, clearly above the world average, at only 6%. According to data released by IRENA (International Renewable Energy Agency), **Western Europe ranked second for investments in renewables** in the period from 2013 to 2018 amounting to $347 billion, 19% of the world total. The installed capacity from renewable sources increased from around 303 GW in 2011 to over 528 GW in 2020, registering an increase of +74% compared to only 10.5% globally. In line with the increase in consumption, **globally produced CO_2 emissions have also increased**, albeit proportionally less (+3.2%) – from 31,291 Mt in 2010 to 32,284 Mt in 2020. The increase is mainly due to emissions from the Asia-Pacific area, which increased by about one fifth over the decade, while the US and the EU contributed with a considerable decrease related to the decarbonisation objectives – -18.9% for the former, -24.7% for the latter.

In order to promote zero emissions and support MSs in their path towards a fair and inclusive transition, in December 2019, the European Commission presented the ambitious communication on the **European Green Deal**. The strategy aims at making energy production and European citizens' lifestyle more sustainable and less harmful to the environment. The Green Deal is divided into a series of macro-actions containing strategies for all sectors of the economy and, in particular, transport, energy, agriculture, construction and industrial sectors. At the same time, the Commission has launched a **European Green Deal Investment Plan** (EGDIP), **mobilising up to €1 trillion**. Since March 2020, the initiatives taken by the Commission have been numerous. These are mainly action plans and strategic documents concerning the multiple areas included in the European Green Deal. Amongst these, a prominent place is held by the **European Climate Law**, aimed at inserting into EU law the goal of climate neutrality by 2050. MSs are not unprepared for this challenge. Over the last few decades, EU countries have increasingly invested in green technologies and in the production of energy from renewable sources. In 2019, renewables represented 13.6% of EU total gross domestic consumption. Of the renewable energy sources, sun and wind energy carry the greatest weight in the European race towards climate neutrality. The **installed electricity production capacity from these two sources amounted to approximately 289 GW in 2019**. Germany takes the lion's share, with 190.8 GW (66% of EU installed capacity) with a value of over five times higher than Spain (36.9 GW), ranking second. Italy, with 31.5 GW installed, ranks third, ahead of France (27.9 GW). Another essential dimension for the challenge of decarbonisation, as well as for strengthening the security of supply, is energy efficiency. The country that consumes the least energy per unit of GDP is Ireland (0.49 GWh per € million), followed by Denmark (0.65) and Malta (0.75). In order to steer the economic recovery in the green direction, in February 2021, the regulation relating to the **Recovery and Resilience Facility (**RRF) was published. This is the key tool of the **NextGenerationEU** package which

aims at mitigating the economic and social impact of the Covid-19 crisis and, at the same time, addressing the long-term challenges of the Union. One of the main conditions imposed by the EU is that the plans drawn up by the MSs contribute substantially to the green transition, as promoted by the Green Deal, and that, therefore, at least **37% of the available resources should be assigned to the green compartment**. According to a comparative analysis of the National Plans presented to the Commission, the country that has devoted the largest share of its funds to the ecological transition is Luxembourg (60% of the available resources), followed by Denmark (59.6%) and Belgium (51.7%).

Reducing emissions is the main objective of EU policies. To this end, the **Emissions Trading System** (ETS) was launched in 2005 and, today, it is one of the cornerstones of Community policies. It has undergone various revisions (phase 4 of the programme runs from 2021 to 2030) and has expanded the number of countries involved and sectors and plants covered. **Verified emissions from stationary installations decreased by 35%** between 2005 and 2019, decreasing at an annual average rate of about 3%, to reach 1.53 Gt C02 equivalent. **Combustion plants have reduced their emissions the most**, despite still accounting for 60% of the total verified emissions. Industrial plants on the other hand, have increased their emissions, on average, by 14% and account for 36% of overall emissions. The ETS reform is, therefore, one of the pillars around which "**Fit for 55**" revolves. This is the package of measures proposed by the European Commission to place the EU on **the path to reducing CO_2 emissions by 55% by 2030**, the first step towards achieving climate neutrality by 2050. "Fit for 55" consists of 16 acts – two communications, four directives, eight regulations and two decisions. The communications concern emission targets for the coming decades and infrastructures for alternative fuels. The directives concern the ETS, renewable sources, energy efficiency and the taxation of energy products and electricity. The regulations relate to **Effort Sharing** (the annual reduction targets of emissions), the **carbon adjustment mechanism at the border** (CBAM), the creation of a Social Climate Fund, the use of soil and forestry (LULUCF), emission standards for cars and vans and infrastructure for alternative fuels, through the revision of the DAFI, air transport (ReFuelEu Aviation), and the use of renewable and low-carbon fuels in transport maritime (FuelEu Maritime). The decisions also propose a notification system for emission offsets for the aviation sector and the ETS market stability reserve until 2030. Overall, in this way, the European Commission wants to review the entire toolbox available to climate policies, setting the bar high for ambitions.

Paragraph 3.2 is focused on **green finance**. The most recent scenario analyses highlight the need to mobilise a considerable amount of funding to achieve the goal of climate neutrality by 2050. The IEA report "Net Zero by 2050: A Roadmap for the Global Energy Sector" quantified **US$5 trillion by 2030 as the investment needed for the energy transition, about 4.5% of global GDP**. Today, investments to achieve climate neutrality are much lower than what is needed. **In 2020, global**

investments in the low-carbon energy transition amounted to $501.3 billion, up from $458.6 billion last year, and from just $235.4 billion in 2010. **The first sector for investments has been renewable energy ($303.5 billion)**, up by 2% compared to 2019 despite some delays due the Covid-19 pandemic. Following, we find electric transport with $139 billion being invested in new vehicles and charging infrastructures (+28%) and electric heating with $50.8 billion in investments (+12%). **Europe and China are currently competing for the most active markets in energy transition investments**. Last year, European countries allocated a large part of the increase in investments in this area. Growth for Europe is +67% compared to 2019, for a total value of $166.2 billion, higher than China and the US. **Europe recorded an increase of 28% in green bonds issued in 2020**, with an overall increase (+$34.5 bln) even higher than the world average (+$23.2 bln). This trend strengthens **European leadership**, with an overall volume, in the 2014-2020 period of approximately $465 billion, almost double that of North America and the Asia-Pacific area.

EU actions to promote sustainable finance are made up of numerous legislative initiatives, which have gradually intensified, particularly after March 2018, when **the Action Plan on Financing Sustainable Growth** was published. Measures in this area have taken on even greater importance following the launch of the European Green Deal, which announced the revision of the **European Strategy on Sustainable Finance**. On March 2020, the final report on the "**EU Taxonomy**" of sustainable economic activities was published. The document classifies the main economic sectors on the basis of their ability to mitigate or adapt to climate change. The first of the delegated acts of the EU Taxonomy, approved by Commissioners on 21 April, introduces a series of technical screening criteria to define the activities mainly contributing to two of the environmental objectives envisaged by the taxonomy regulation – the adaptation to climate change and climate change mitigation. A second delegated act covering the remaining targets will be published in 2022. The EU sustainability disclosure obligations will be extended to all large or listed companies, so that nearly 50,000 companies in the EU will have to comply with detailed standards, compared to the 11,000 currently subject to current obligations.

The Commission is aiming to raise 30% of the €750 billion of resources needed to finance NextGenerationEU on the markets through the issuance of green bonds. The first issue recorded a demand for more than €135 billion, compared to the 12 billion of securities issued. An important role in the European context of sustainable finance is played by the European Investment Bank (EIB), which already, in 2007, had launched the first green bond – the Climate Awareness Bond.

Paragraph 3.3 analyses the decarbonisation of the **transport sector**. Reducing the pressures of transport on the environment and climate is key to achieving the long-term vision of EU zero emissions by 2050. Over the last decades, emissions from the EU transport sector have not been dropping enough to limit its environmental

and climate impacts. Nowadays, **it represents almost a quarter of Europe's greenhouse gas emissions** and is the main cause of air pollution in urban areas. The average age of cars on EU-27 roads is 11.5 years, meaning that more than **half of the cars currently used by European citizens were purchased before the introduction of the Euro 5 emission standard**. Despite an increase in registrations in recent years, alternatively-powered cars make up just 4.6% of the total EU car fleet. Only 0.8% of all cars on Europe's roads are hybrid electric, while both battery electric and plug-in hybrids each account for only 0.2% of the total. In 2019, almost 60% of all new cars registered in the EU ran on petrol

In addition to the **Sustainable and Smart Mobility Strategy**, the transformation of mobility and transport systems also finds its place in other papers from the European Green Deal – e.g. "**A Hydrogen Strategy for a climate neutral Europe**" aims to boost clean hydrogen production in Europe. The **IPCEI "Fuel Cells and Hydrogen"** funded by Horizon 2020 seeks to accelerate European technological progress in this area. The European Commission is also pushing for the development of electric batteries, key enabling technology for the ecological transition and central to European automotive competitiveness. To this end, in 2017, the Commission had already launched the **European Battery Alliance** (EBA) in agreement with the EIB, EU countries, industry and the scientific community. Recently, the Commission approved a second IPCEI to support research and innovation in the battery value chain prepared jointly by 12 MSs for a total value of €2.9 billion in funding until 2028. This should mobilise €9 billion in private investments, contributing to EU autonomy in the sector.

PART

DIGITAL

1. DIGITAL

1.1. THE ROLE OF PLATFORMS IN THE MARKET. THE DIGITAL MARKETS ACT (DMA) PROPOSAL

1.1.1. Digital market complexity and dynamism in the convergence era

The spread of digital services has brought obvious benefits to users and has contributed to fostering the development of domestic markets by creating new business opportunities and facilitating international exchanges. Digital services enable us to carry out a wide range of activities that have become a part of everyday life, including the use of marketplaces, social networks, search engines, as well as online brokerage services or applications for a variety of uses (work, games, free time, sharing). These all increase the possibilities of consumption, improve the efficiency and competitiveness of the industry and make it easier to participate in civil society.

The growing importance of the digital market can be seen as one of the most important changes of our era, since it is an enabling element for economic growth and a driving force for transforming daily activities. At the same time, the analysis of this type of sector is extremely complex, due to its blurred boundaries and high degree of dynamism and innovation. Indeed, digitalisation makes it difficult to identify clear definitions on the boundaries of individual market segments (such as the definition of the relevant market). Digital services are constantly changing, adapting to the context, adding new functionalities and bringing competition to a multi-dimensional level that is developing at the same time on multiple fronts. The speed market trends change is also an element that further complicates the analysis, making it difficult to produce accurate forecasts on the development of a sector and the possible impact of policy intervention. Furthermore, demanding challenges arise for the companies that compete with each other, pushing them to continuously evolve requiring (for those with the availability) investments to improve technologies and services, accelerate and further alter the market dynamics. In this perspective, sectors such as e-commerce, application stores, social platforms and online advertising are examples of the changing environment the different areas of the digital market move in.

In recent years, **e-commerce** has undergone a marked boost in terms of both sales and turnover, becoming an essential component of the global retail trade. Many companies around the world have adopted business solutions to allow for the sale of their products online, both with and without the support of marketplaces, in order to expand their national and international user base. The pandemic has further accelerated this trend, as social distancing measures and confinement have pushed most consumers, even the most reluctant ones, to change their shopping habits in favour of the online channel.

On the other hand, **in absolute terms, e-commerce still seems to have a limited impact on national economies**, particularly in contributing to GDP. For example, data published by Statista and the World Bank[3]

3 Statista Digital Market Outlook del 2021

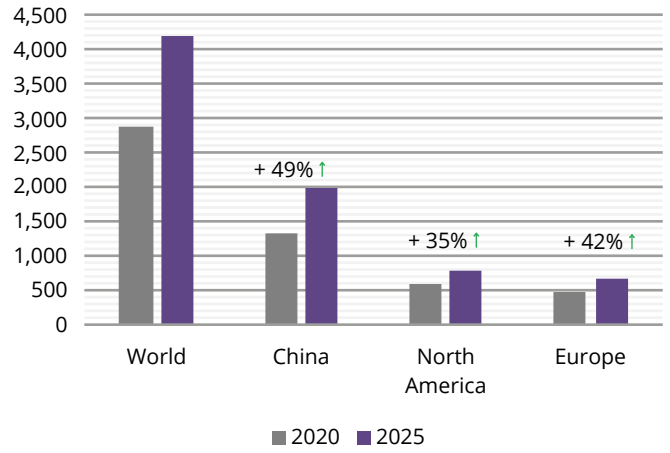
shows that in China alone consumers spend more than 10% of national income online (2020), while in European countries this is significantly lower (in the UK at 4%, in Poland 3.7%, in Germany 3%, in Italy 1.9%), as well as in the United States (2.6%).

An important role in the remarkable growth of the sector is played by the large digital marketplaces. These platforms have reached a global dimension and are used by a huge mass of consumers. At the same time, it can be observed how the distribution of market shares greatly differs between geographical areas, benefiting companies that are better able to satisfy the tastes and needs of the local citizens. For example, while Amazon is the most important digital marketplace in Western countries, it has achieved a much lower share in Latin America, where the MercadoLibre[4] platform excels in markets such as Brazil, Mexico, Argentina, Colombia and Chile, managing approximately 86% of online sales in South America. The situation is similar in Asia, particularly China, where the US marketplace, as well as eBay, has been almost completely eclipsed by local players such as Alibaba / Aliexpress, JD and Suning, while Amazon China has a market share of less than 1%.

In Europe, where Amazon is the main platform, it receives half of monthly web visits (1.1 billion) compared to the US (2.3 billion), even if the two areas are similar in population and GDP and not too different in e-commerce penetration. This can be considered as a result of the increased competition that non-EU companies face in

Fig. 1.1.1 E-commerce sales in major areas of the world ($ bln)

Source: Statista 2021



European markets, where players such as the German Zalando, the English Asos, the French Cdiscount[5] are gaining in market share compared to the large US companies Amazon and eBay (although in the US, traditional digital converting companies such as Walmart and Target are increasing dramatically and very quickly). In 2020, the **volume of sales generated globally from online purchases** amounted to $2.855 billion, while estimates foresee the total turnover to grow by 47%, reaching $4.200 billion in 2025. It is the Chinese market expected to grow the fastest, with forecasts indicating a 49% increase in sales volume between 2020 and 2025 (from $1.344 billion in 2020 to $1.996 billion in 2025).

4 https://seekingalpha.com/article/4372121-mercadolibre-tale-of-two-markets

5 The PriceMinister platform was acquired by the Japanese Rakuten, of which it currently bears the name.

North America follows, with online sales expected to increase by 35% over the period considered, reaching a value of $794.6 billion in 2025. Europe is at the bottom of this close ranking, with an estimated growth of 42%, amounting to $656 billion (Fig.1.1.1). If this trend is confirmed, in 2025, the Chinese e-commerce market will become about 2.5 times larger than the US market and even 3 times larger than the European.

A branch of the digital market that has become quite important in recent years is the **mobile sector**. According to the latest data released by GSMA Intelligence, about two thirds of the world population currently uses a mobile phone, about 85% of all people aged 13 and over. In just a decade, the smartphone has become an indispensable tool in the daily lives of millions of people, with penetration rates reaching 78% in Europe and 82% in North America (73% in China). GSMA estimates that, in 2022, 6 million citizens globally will own a smartphone.

At market level, on the hardware production side, the sector is extremely dynamic and competitive, with Samsung having seen its market shares decrease (from 19.5% to 18.8%) to the advantage of Apple (which rose to 14.1, +17.8% compared to June 2020). However, above all, the Chinese company Xiaomi has climbed to second place with a 16.9% market share, overtaking Apple. In June 2021, Xiaomi recorded a volume of shipments almost doubled YoY (from 28.5 to 53.1 million products distributed), a growth of 86.6% (Tab.1.1.1).

The situation for the **software market** is different, especially regarding operating systems. Over the last decade, the market has been reduced to just two main suppliers, creating a duopoly – Google Android (Alphabet) and iOS (Apple) together representing 99% of the market. Therefore, a progressive evolution can

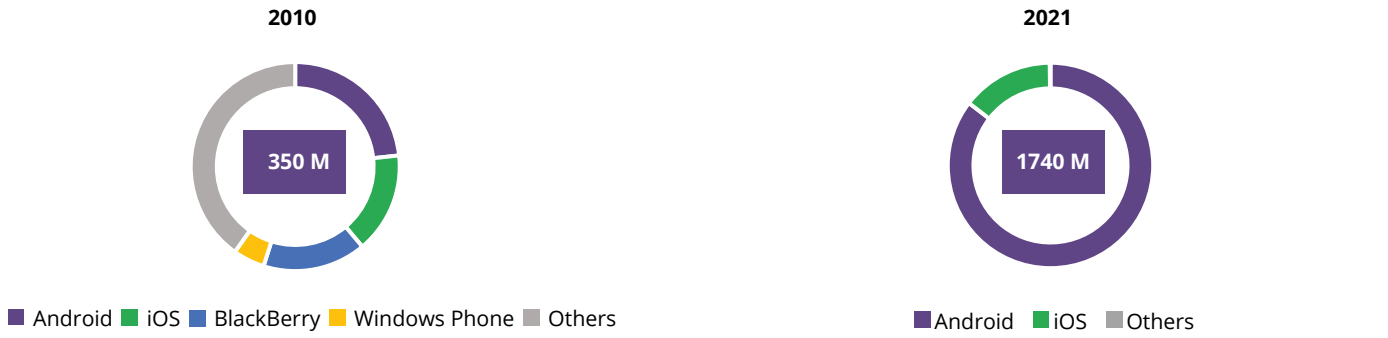
Tab. 1.1.1 Top 5 smartphone companies worldwide (in mln devices shipped)

Source: IDC Quarterly Mobile Phone Tracker, July 2021

Company	2Q21 Shipping	2Q21 Market share	2Q20 Shipping	2Q20 Market share	Δ% YoY
Samsung	59.0	18.8%	54.0	19.5%	9.3%
Xiaomi	53.1	16.9%	28.5	10.3%	86.6%
Apple	44.2	14.1%	37.6	13.6%	17.8%
OPPO	32.8	10.5%	24.0	8.7%	37.0%
Vivo	31.6	10.1%	23.7	8.6%	33.7%
Others	92.4	29.5%	109.0	39.4%	-15.2%
Total	313.2	100.0%	276.6	100.0%	13.2%

Fig. 1.1.2 The evolution of the operating systems market share

Source: I-Com elaborations on IDC data



be witnessed compared to the 2010 scenario, when Windows Phone and Blackberry were also active and the Android – iOS duo had not exceeded 39% of the market (Fig. 1.1.2).

Analysing the use of the two operating systems for each country, it is interesting to note how Google Android is the most used worldwide as it is designed to be compatible with the hardware of multiple manufacturers. However, as evidence of the complexity of technological competition, it is also worth highlighting how in Japan and the US, two of the world's most advanced markets, Apple is the leader with a share of around 50% of users. On the other hand, the widespread use of Google-owned software stems from its open-source nature, allowing it to be used on a wider range of hardware and to develop new operating systems (although other versions based on the Android source code never seem to have really caught on). Here, the actual effect of pre-installing software and apps on devices is still unclear in terms of actual usage. While, on the one hand, Google is under investigation[6] for the distribution of the apps of the Google Play Service and its most widespread and characteristic services (Google Search, Gmail, Google Maps, Chrome, Google Play Store, YouTube), on the other, the number of downloads and the use of these apps even on rival devices (e.g., YouTube, Google Maps and Chrome are among the most downloaded apps even on Apple's AppStore) show that some leading services are spreading. This is due to their excellent performance.

Closely related to operating systems analysis is the **app market**. These are of key importance in the smartphone market, allowing an individual to use the same tool for countless functionalities. For this reason, apps are the services that mobile users spend most of their time nowadays. Based on some estimates made in January

6 The case is T-604/18 Google vs the European Commission. The hearing was closed on 4 October, although, at present, the timing of publication of the verdict is not known.

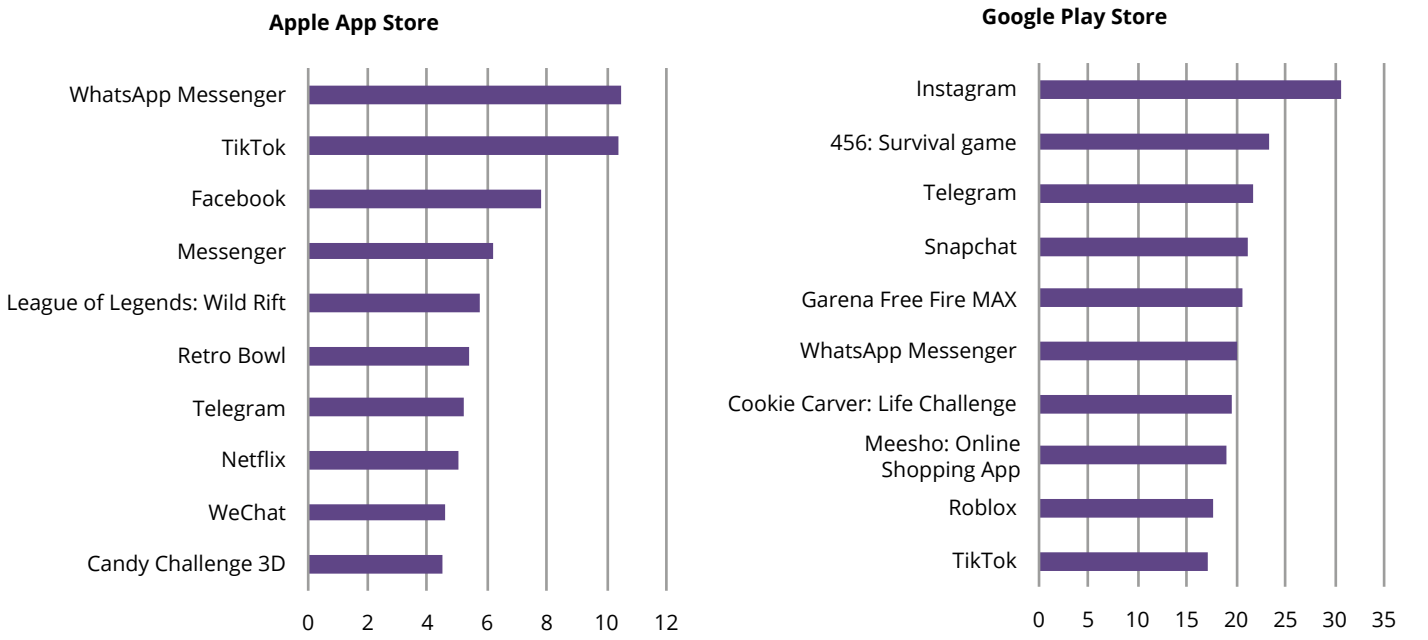
2021 on a panel of Android users, the time spent on mobile devices exceeds an average of 4 hours a day, 44% being dedicated to sharing content, communication and social media, while 26% for entertainment and video apps and 9% video game apps.

By observing the data released by Airnow on the most downloaded apps worldwide from Apple and Android stores in October 2021, it can be seen how, among the apps with the highest number of users, there are all those that refer to social media (Fig.1.1.3). The Meta group apps (Facebook, WhatsApp, Instagram, Messenger) are the most downloaded (75.42M), but also those of other social networks such as TikTok (27.44), Telegram (26.3) and Snapchat (21.1) record an excellent performance.

However, when analysing the number of downloads compared to the different stores (App Store for iOS and Google Play for Android), it must be remembered that many of the main apps are pre-installed in some types or versions of operating systems and, therefore, present without having to be downloaded. Consequently, this factor tends to alter the relationship between the number of downloads and effective spread of the apps. As seen

Fig. 1.1.3 Top 10 downloads worldwide in October 2021, by store (in mln)

Source: Airnow



previously, this is the case with many of Google's apps, but is also now the case with the most popular social media apps, entertainment platforms and leading e-commerce apps.

Net of these considerations, at the level of global downloads, 2020 showed significant growth rates, both for absolute downloads (+7% on 2019) and spending per app (+20% on 2019). During the year, the most downloaded app worldwide was, for the first time, TikTok. Despite the geopolitical obstacle posed by the Trump Presidency, the Chinese app managed to overtake WhatsApp, which had led the ranking in 2019.

Where the **social network segment** is concerned, it can be observed that it includes a wide range of services that sometimes have quite different characteristics. While most of these allow users to connect, communicate and share content of a different nature (texts, images, videos and even direct streaming), they differ in other features, such as the type and scope of the exchange, public or private (both text, voice or audio-visual) in real time, the ability to create groups and communities online. Still others offer more focused services, for example, by focusing on specific aspects (e.g., publishing and sharing images and / or videos).

In particular, market dynamics show how "classic" social networks (e.g., Facebook), video sharing platforms (YouTube, TikTok) and personal communication media (WhatsApp, WeChat, Telegram) are actually in direct competition with each other, and aim to expand or reposition their offer of services meeting as much as possible public tastes, gaining new users by enticing them away from rivals and prolonging the time of use. Consequently, **the definition of these platforms tends to transcend the boundaries of such categories, complicating the analysis and making it difficult to provide a clear and comprehensive picture of the sector and its sub-categories**.

The main examples of this are Facebook (now, Meta) and Google, which initially competed with each other in the social network sector (before the disappearance of Google +), and which now also compete directly in the digital advertising and video market, and also with TikTok in the video sector and in social networks. The trend towards expansion and integration of new features has reached one of its peaks in China with WeChat, a platform that has created an ecosystem that also includes payments via smartphone. A similar strategy, if reproduced in Europe and the US by WhatsApp (or by Facebook itself), could lead to an even higher level of diversification and complexity.

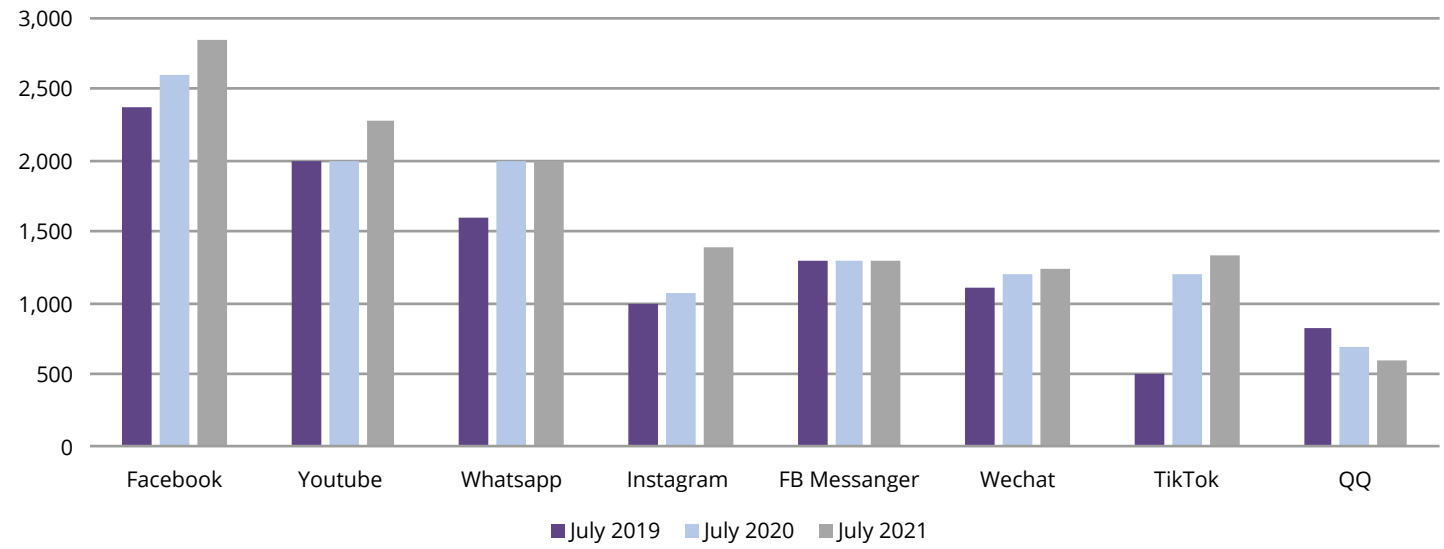
The macro analysis of the social network market focuses more generically on the number of users, a measure that provides an explanatory idea of global trends. The turnover linked to the platforms depends on factors such as the ability to attract as many people as possible and the quantity and quality of data they are able to collect, since revenues are closely linked to advertising services. With borders disappearing, analysts usually group video sharing applications, communication services and hybrid providers into a single category in order to address this complexity. According to the analysis of Kepios, for example (Fig. 1.1.4), in 2021

the social media with the highest number of users is still Facebook, with about 2.9 billion users (+20.1% compared to 2019), followed by YouTube with 2.2 billion users in 2021 (+14.6% in two years), WhatsApp (2 billion users) and Instagram (1.4 billion users). At 1.2 billion total users is TikTok[7] which, launched in 2016, quickly climbed the market rankings thanks to the innovative video sharing service, managed by very advanced AI algorithms, offered in a user-friendly format and designed to increase usage time.

Focusing on the data concerning the net growth of the Chinese social network (Fig.1.1.5), the speed of its spread is evident. Between 2019 and 2021, the app recorded a growth of 166.4%, conquering more than 830 million monthly active users worldwide. In this period of time, TikTok has therefore gained almost 400 million users more than Facebook (which also won over a further 480 million), about 450 million more than Instagram, (+386 million) and about 750 million more than Twitter (+67 million) and 700 million more than Reddit (+100 million). This once again shows the high permeability and the very high level of competition of a market that remains open to innovative technologies and more user-friendly interfaces.

Fig. 1.1.4 Active users globally on social platforms (in mln)

Source: Kepios Analysis, Hootsuite and We are Social, 2021

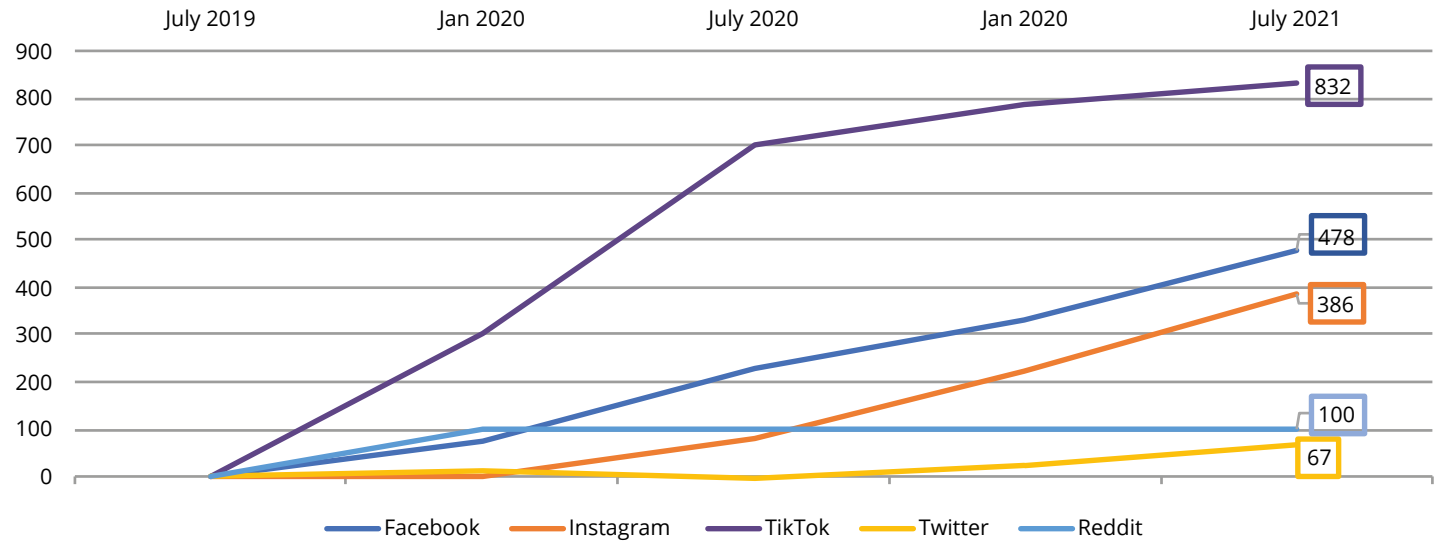


Note: Based on recently released platform data, TikTok includes both TikTok and the Chinese version, Douyin.

7 TikTok and Douyin together

Fig. 1.1.5 Net growth of monthly active users in major digital platforms (in mln)

Source: Kepios Analysis, Hootsuite and We are Social, 2021



Note: Based on recently released platform data; TikTok includes both TikTok and the Chinese version, Douyin

1.1.2. The Digital Markets Act proposal and latest developments

To regulate the new critical issues connected to the affirmation of large online intermediaries and platforms, on 15 December 2020, the European Commission submitted the **Digital Markets Act (DMA)** which represents one of the most important milestones of the EU digital strategy. The regulation is focused on 8 "core platform services"[8]: 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 (art.3) requires 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

8 Seven principal and one accessory (advertising services which will be regulated only when offered by a provider of any of the principal CPSs).

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 MSs;

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;
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 reelation 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.

1.1.3. The European debate on the DMA proposal

The DMA proposal has triggered a wide-ranging debate among stakeholders and numerous requests for change. The debate focuses on the new obligations that will fall upon actors as well as the new powers, some of which are deemed to be too very pervasive, that the Commission will be granted if the DMA is approved in its current form. Therefore, it is worth reconstructing the essential contents of the positions expressed at MS, institutional and market level.

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.

In general, the **Body of European Regulators for Electronic Communications (BEREC)** 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.

The **Presidency Report** of 17 May 2021, offers a detailed examination of the positions expressed by the Member States on the general architecture, scope and substantial provisions, as well as the overall enforcement system of the DMA. In general, the report has recognised broad support for the need to balance speedy and flexible procedures with legal certainty of the measures, the combination of quantitative and qualitative thresholds for designating gatekeepers and the importance of effective investigative instruments, supported by effective sanctions. Specifically, the report recognises the positions expressed by MSs on the following topics: **1) role of MSs in the enforcement of the DMA.** Even if the central role of the Commission is welcomed, MSs call for further consideration of their role – including competent national authorities, for example in the opening of market investigations, market monitoring and in the decision-making procedure – and for clarifying the framework for cooperation and information sharing between the Commission and MSs; **2) Delegated acts.** Some MSs expressed some doubts about the scope of delegated acts envisaged in the proposal and reservations regarding the use and scope of delegated acts for the update under art. 10 of obligations laid down in art. 5 and 6, including in light of the rules applicable to the adoption of delegated acts. **3) Scope, legal basis and interplay of DMA with other legislation.** Several MSs have called for more clarity

regarding the coordination between the Digital Markets Act and other EU and national rules. **4) Designation of gatekeepers, obligations and regulatory dialogue.** MSs generally support the key principles of the mechanism to designate gatekeepers, in particular, the combination of quantitative and qualitative criteria even if some states have proposed changes to the criteria defining the designation procedure, other states raised issues relating to the deadlines applicable to the market investigations concerning the gatekeeper designation or called for adjustments to the scope and conditions of some of the obligations set in art. 5 and 6 (obligations concerning interoperability, data portability and access to data) and the adoption of a more individualised approach. Some MSs have also highlighted the need to clarify the interplay between the regulatory dialogue framework and non-compliance proceedings.

At the end of May 2021, the governments of France, Germany and the Netherlands published a non-paper, the "***Friends of an effective Digital Markets Act***". It claims that the scope of the DMA should be targeted, taking into account the role of ecosystems 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 MSs 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 calls 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. After the publication in May of this common position paper, on 7 September 2021, the governments of France, Germany and the Netherlands published a **working paper on Strengthening the Digital Markets Act and its Enforcement**, containing some amendments. Specifically, considering the necessity to ensure more future-proof and tailor-made remediation to cope with the reality of digital markets, the paper welcomes the speed that the self-executing obligations in art. 5 and 6 of the DMA provide but underlines that adding further intervention possibilities to the lists in these articles might not be proportional and could risk harming innovation. To maximise speed and legal certainty within this mechanism, the paper calls for the adoption of a decision by the Commission based on a pre-defined list of a limitative set of principle-based measures – to be chosen from access to platforms, data-related interventions, fair commercial relations and end-users and business-users open choices – tailored to what is needed for a specific gatekeeper. It proposes that

obligations would only be imposed if the preliminary results of the market investigation showed that the existing obligations in art. 5 or 6 are not sufficient to ensure fairness and market contestability in the precise case under investigation and that competition law alone is insufficient to adequately and timely address the identified practices. Instead, for the role of national authorities, starting from the consideration that enforcing the DMA will need staff with expertise to match the resources of the gatekeepers, the paper calls for the support of national competition authorities to the Commission, within a referral system similar to the one currently already in use in merger control. Specifically, the Commission and national competition authorities should closely cooperate and coordinate their actions via the European Competition Network to ensure a swift and effective enforcement and an optimal allocation of the workload at European and national levels. Finally, the working paper underlines the purpose of the DMA to contribute to the proper functioning of the internal market by laying down harmonised rules ensuring contestable and fair markets in the digital sector and highlights that the centralisation of certain powers at EU level, such as gatekeepers' designation or regulatory dialogue with gatekeepers, is able to improve effectiveness and prevent fragmentation.

On 1 June 2021, the 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), suggesting the following main modifications: **1) definition and designation of gatekeepers.** The Report proposes to increase the quantitative thresholds and to add – as an additional condition for companies to be designated as gatekeepers under art. 3(2) of the Regulation – that they are providers of not only one but, at least, two core platform services (thinking that the provision of two or more core platform services is 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 art. 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 art. 3(2). The report also underlines the importance of guaranteeing a fast and efficient application of this regulation and legal predictability also adding a list of indicators as an Annex, in order to clarify how to establish the number of monthly active end-users and yearly active business users for the purposes of art. 3(2); **2) obligations and prohibitions.** The report welcomes 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, even if it suggests the clarification of self-executing nature of the obligations and prohibitions foreseen in the regulation. 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 art. 5 and 6; **3) market investigation and structural remedies.** The report underlines the importance of the national authorities support to the Commission in market investigations activities for the designation of gatekeepers. In addition, on the imposition of structural remedies the same report proposes that it 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 MSs, the Commission, as well as any relevant EU bodies and other representatives of competent authorities in specific sectors – which 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 and facilitate cooperation and coordination between the Commission and MSs in their enforcing decisions, in the interest of a consistent regulatory approach.

In the same month, June 2021, national competition authorities published a **joint paper** asking for more involvement in the enforcement of upcoming competition rules. France, Germany and the Netherlands, in particular, proposed two amendments – the first, to introduce the possibility to impose tailor-made obligations, and the second, to reinforce the role of the national authorities.

The Committee on the Internal Market and Consumer Protection (IMCO) and the Committee on Economic and Monetary Affairs (ECON) adopted their opinions in June and July 2021. while the Committee on Civil Liberties, Justice and Home Affairs (LIBE), the Committee for Industry, Research and Energy (ITRE) and the Legal Affairs Committee (JURI) all adopted their opinions in September 2021.

1.2. THE NEW REGULATORY FRAMEWORK ON DIGITAL PLATFORMS

1.2.1. The Digital Services Act (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. The DSA proposal is a horizontal instrument that aims to create a safer and trusted online environment. It puts in place a framework of layered responsibilities targeted at different types of services (i.e., intermediary, hosting, online platform, and very large online platforms services) and proposes a set of harmonised EU-wide asymmetric obligations to ensure transparency, accountability and regulatory oversight of the EU online space (for more information see below the briefing on the Digital Services Act: EU Legislation in Progress).

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.

1.2.1.1. Categories of providers and liability exemptions

The proposal identifies several types of providers: a) **"mere conduit" services (art. 3),** involving the transmission in a communication network of information provided by a service recipient, or the provision of access to a communication network. The service provider is not liable for the information transmitted, if it 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. 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)** involving transmitting, over a communications network, information provided by a service recipient, 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 it: (i) does not modify the information; (ii) complies with the conditions of access to the information; (iii) complies with the rules for updating the information, according to the rules of the industry; (iv) 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 exercising of the afore-mentioned activities, prevent or put an end to the violations committed; c) **"hosting" services (art. 5)** involving the storage of information provided by a service recipient where the service provider is not liable for the information stored at the request of a recipient of the service when 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.

1.2.1.2. 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 MSs** 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 MSs, divided on the basis of the type of illegal content they relate to, 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. Specifically concerning 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 information (including the precise indication of the URL

or URLs) where 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 to 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 recipien'ts 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 service recipient 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 MS/MSs 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 MS 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 MS 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 giving 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 it is displayed, the period during which it was displayed, whether it 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.

1.2.1.3. Governance structure and penalties

In defining the **structure of governance**, the proposed regulation requires MSs 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 regulation violation by the large platforms. Where violations committed by large platforms are concerned, the regulation specifically 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 MS where the supplier's head office is located, while for suppliers not established in the Union, the MS 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 MS authorities, the Community institutions and civil society organisations. It will set 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 MSs 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.).

1.2.1.4. The debate on the proposal

The DSA proposal to redesign the role and responsibilities of platforms and produce a strong impact on platforms, has triggered a wide debate among stakeholders.

On 10 February 2021, the **European Data Protection Supervisor (EDPS)** published its opinion on the European Commission's proposals for a Digital Services Act welcoming the proposal that seeks to promote a transparent and safe online environment, and recommending additional measures to better protect individuals when it comes to content moderation, online targeted advertising and recommender systems used by online platforms, such as social media and marketplaces. The EDPS has also highlighted that any form of content moderation should take place in accordance with the rule of law and profiling for the purpose of content moderation should be prohibited unless the online service provider can demonstrate that such measures are strictly necessary to address the systemic risks explicitly identified in the Digital Services Act. Furthermore, the EDPS calls on European legislators to consider a ban on online targeted advertising based on pervasive tracking and restricting the categories of data that can be processed for such advertising methods.

In the Council, discussions to find a common position on the DSA have started and the Portuguese Presidency issued a progress report on 12 May 2021. It underlined the importance to preserve the main principles of the e-Commerce Directive and the need for effective implementation. To this end, the same position has called for a better clarification of the mechanisms for cooperation and coordination with the Commission and a greater involvement of the country of destination. MSs have also underlined the need to harmonise the due diligence obligations and the exemptions from liability for providers of intermediary services. Furthermore, MSs broadly supported the new notice-and-action

procedures and redress mechanisms for users, and the fact that the proposed regulation refers to illegal content as defined by national or EU law. They also supported the asymmetric approach of the proposal, introducing graduated obligations for service providers subject to their size and the impact of their services.

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 also proposes several amendments. Specifically, the most important 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 art. 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 MSs. 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 service recipients. The report proposes a new article that allows service recipients to choose the communication means with the intermediary services. Lastly, according to the report, the additional obligations imposed on online

platforms under the Regulation's Chapter 2, Section 3, 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, they 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.

The Committee on Civil Liberties, Justice and Home Affairs (LIBE), the Committee for Industry, Research and Energy (ITRE) and the Legal Affairs Committee (JURI) are associated committees. The LIBE Committee, the ITRE Committee, the JURI Committee, the Culture Committee (CULT), the Committee on Transport and Tourism (TRAN) and the Committee on Women's Rights and Gender Equality (FEMM) all adopted their opinions in September and October 2021.

While MSs are generally supportive of the proposal, in-depth discussions continue on a number of contentious points (e.g., enforcement and enforceability, content moderation) to find a common position. The Council was informed of progress achieved so far in the examination of the proposed regulation at the Competitiveness Council of 27-28 May 2021. The Portuguese Presidency circulated a first compromised text on 16 June 2021. The Slovenian Presidency circulated a new compromise on Chapter 1 (General provisions) and 2 (Liability of providers of intermediary services) on 2 September 2021.

Several requests for changes have also been made by providers and representative bodies. In particular, there have been requests to rethink the type of obligations imposed on suppliers in view of their practicability and sustainability and in consideration of the impact on security and specific business models. They also requested to strengthen regulatory dialogue to customise obligations and sanctions, to extend some obligations, especially those for the protection of consumers, also to SMEs, to strengthen and extend certain requirements on online advertising, to reinforce the obligation to trace traders by extending the scope of certain provisions to all intermediary services and by introducing new provisions aimed at online markets, to set stricter deadlines for taking action on high-impact content and to clarify the concept of illegal content in order not to undermine the harmonisation efforts made with the proposed framework.

1.2.2. The regulated sectors. An overview

1.2.2.1. Market places, e-commerce and protection from fraudsters on the web

The debate about the DSA takes place in the context of a growing e-commerce market. Volume of activities and revenues linked to online shopping have been growing for years, but the pandemic has drastically accelerated the process. Limitations imposed by the health emergency have boosted digitalisation pushing many people to approach digital platforms for the first time. E-commerce has not been left out in this trend as new users have been attracted by the possibility of purchasing online goods and services that otherwise they could not access during the pandemic. To realize the huge impact that Covid-19 has had on this sector, it is worth noting that 76.8% of the population interviewed by Global Web Index, answered 'yes' when asked if they had made any type of purchase

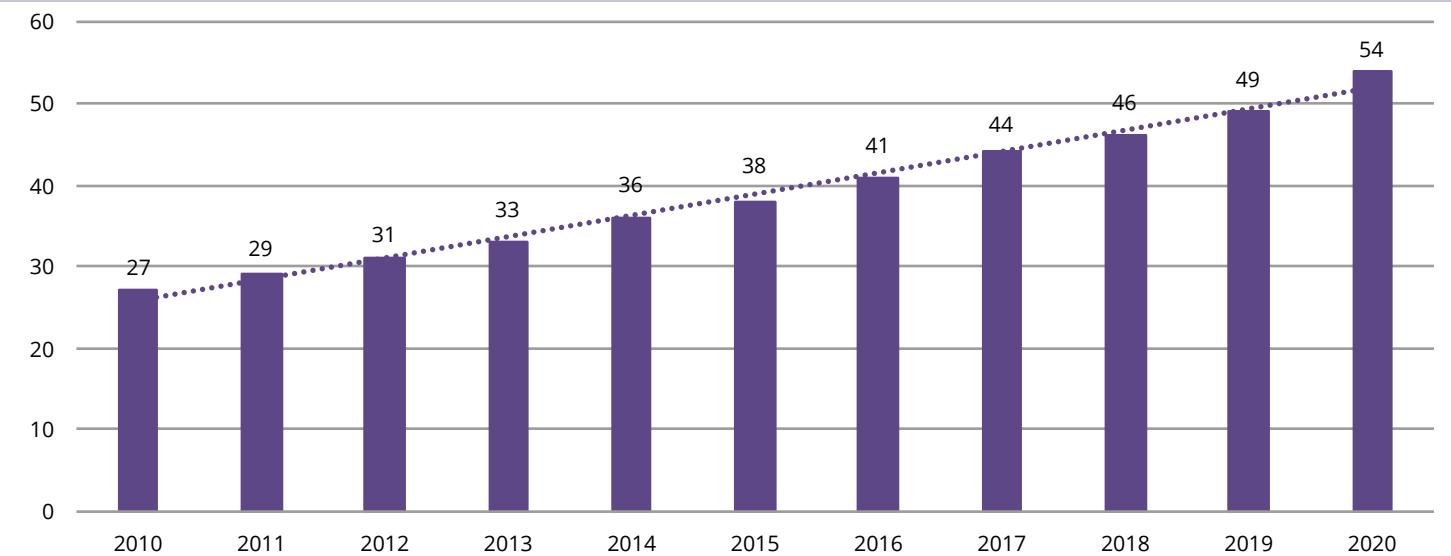
online, on any platform, in the past month with reference to the third quarter of 2020.

E-commerce volume of activities in terms of online purchases has steadily increased during the last decade in Europe. Eurostat data shows that the percentage of individuals that bought online at least one good or service within the last three months[9] rose in the European Union (EU-27) from 27% in 2010 to 49% in 2019, recording a 5 percentage points jump in 2020, up to 54% (1.2.1). The countries in the highest-ranking positions are Switzerland, Denmark and Germany, with a share of the population that exceeds 70%, while Italy, at 28%, is placed well below the European average.

One of the main issues linked to the thriving e-commerce concerns the increase in bad actors and fraudsters on the web. The rise in the number of people purchasing goods and services on the Internet driven by the pandemic resulted in the modification of the consumer base. Plenty of new non-tech-savvy users approached digital services for the first time, hence becoming an easy target for fraud and abuse. As a result, illicit acts have prospered, pushing authorities and companies to look for new strategies to counteract the problem.

Fig. 1.2.1 Percentage of individuals that made their last purchase online in the last 3 months*

Source: Eurostat



** Data refers to the first quarter of the reference year*

9 Data refers to the first quarter of the reference year.

According to Federal Trade Commission data, US citizens have lost more than $145 million because of frauds related to Covid-19, while Google recorded a 250% increase in phishing websites between January and March 2020. Nevertheless, customers seem not to be so willing to succumb to the bad actors as, according to Marqueta's 2020 Fraud Report, almost 87% of the sampled population would accept transactions to take longer if this meant better protection. 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.

Web frauds are of different natures. In particular, Account Takeover Attacks (ATO), i.e. identity thefts used to gain unauthorised access to accounts, rose by 282% between 2019 and 2020. Chargebacks are very common and represent between 40-80% of web frauds. Phishing websites also rocketed during the pandemic and 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 on the web has led to a transformation in how consumer protection is handled. The trend is to move from a defensive approach to risk intelligence models that work as business optimisation engines. Moreover, due to the large amount of data involved in the management of large platforms, machine learning technologies are becoming popular to support human investigation activities that, if performed alone, would require large time spans incompatible with platform needs.

For its part, Amazon has published the Brand Protection Report outlining its strategy to protect customers and stores from fraud and abuse. The company built a hybrid system (made of both human activities and AI tools) to check identities of potential selling partners and developed the Payment Service Provider Program in order to secure transaction by asking specific requirements and compliance controls from payment service providers. Moreover, Amazon decided to engage directly with brand owners in the fight against counterfeited products and enabled them to report suspected infringements and eliminate risky listings from the stores. In addition, the Amazon Counterfeit Crimes Unit aims at stopping bad actors and 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 far as Ebay is concerned, the company relies on two Protection Programmes, the former targets consumers and guarantees them a full refund in the case of unsatisfactory products, while the latter concerns sellers

and protects them in the case of unfair negative feedback in protected sales. Furthermore, eBay developed a software system called FADE (Fraud Automated Detection Engine) in order to fight abuses. The system gathers data from defrauded users and then alerts the company if similar patterns are identified in the context of a new auction. Red flags may coincide with new clients with huge amounts of expensive merchandise, sudden modifications in seller behaviour or an address linked to a country with a high incidence of eBay fraud.

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. Also in this case, this implies the need to process huge quantities of data on the platform. As a result, Zalando's Data Engineering Department estimates the risk of a customer's order by using machine learning models using historical order data. To provide a platform-ready fraud-assessment system, they use the Apache Spark Big Data processing framework that distributes data processing tasks seamlessly to a set of worker machines, which then work in parallel on their own fraction of data. This means that it is possible to seamlessly scale up processing power and memory.

In conclusion, even if the increase in digitalisation due to the pandemic has led to a significant rise in the number of abuses and misbehaviours by digital players, it would be unfair to overlook the huge net benefits that it has brought about and will keep bringing to end-users worldwide. Often, the digitalisation process that a community has to go through, comes with heavy costs in terms of displacement. However, the availability of unprecedented opportunities opened up 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. This is especially so for SMEs that have had huge barriers to scaling up in the traditional economy. Of course, large platforms are instrumental in maximising these benefits, matching businesses with consumers at higher and more efficient levels. **Therefore, the policy objective should be, on one hand, ensuring that fair conditions always apply to digital transactions and, on the other, that innovation is not stifled either by a stable monopolisation or over-regulation.**

1.2.2.2. Social networks, video-sharing platforms and the fight against harmful content

The spread of social networks is revolutionising our way of communicating 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.**

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.

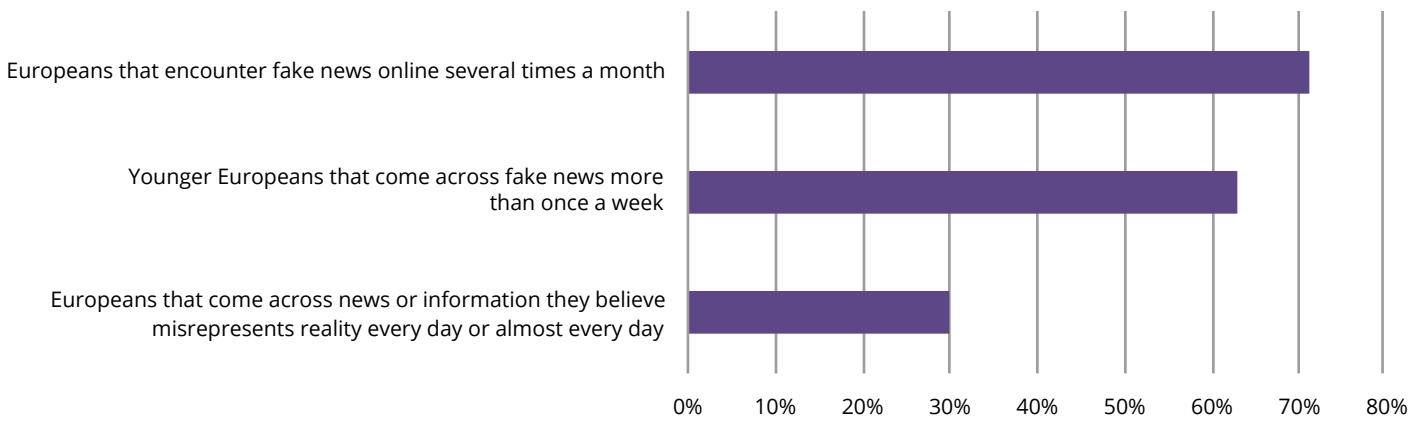
In this scenario, large platforms today play a key role in distributing and shaping information online, assuming a responsibility that, although not definable in typical editorial terms, seems to go far beyond the mere technological aspects. For these reasons, their design choices and security practices strongly influence user safety online, with the power to shape online content 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 a careful moderation and monitoring of published content.

Online misinformation and disinformation

Online misinformation and 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 make informed decisions. According to the latest data of Eurobarometer (Fig.1.2.2), 71% of Europeans encounter fake news online several times a month (30% every day). Those who seem to be most

Fig. 1.2.2 Eurobarometer disinformation data (%, 2018)

Source: Eurobarometer



exposed are young people, which in 63% of the cases say that they encounter 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 16 digital platforms, including leading players of social networks and the advertising industry. 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.

In September 2020, the Commission published 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 platforms have ramped up 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. Facebook and Instagram reported that more than 2 billion users visited their Covid-19 "Information Centre", 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. 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. 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 MSs 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.

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.

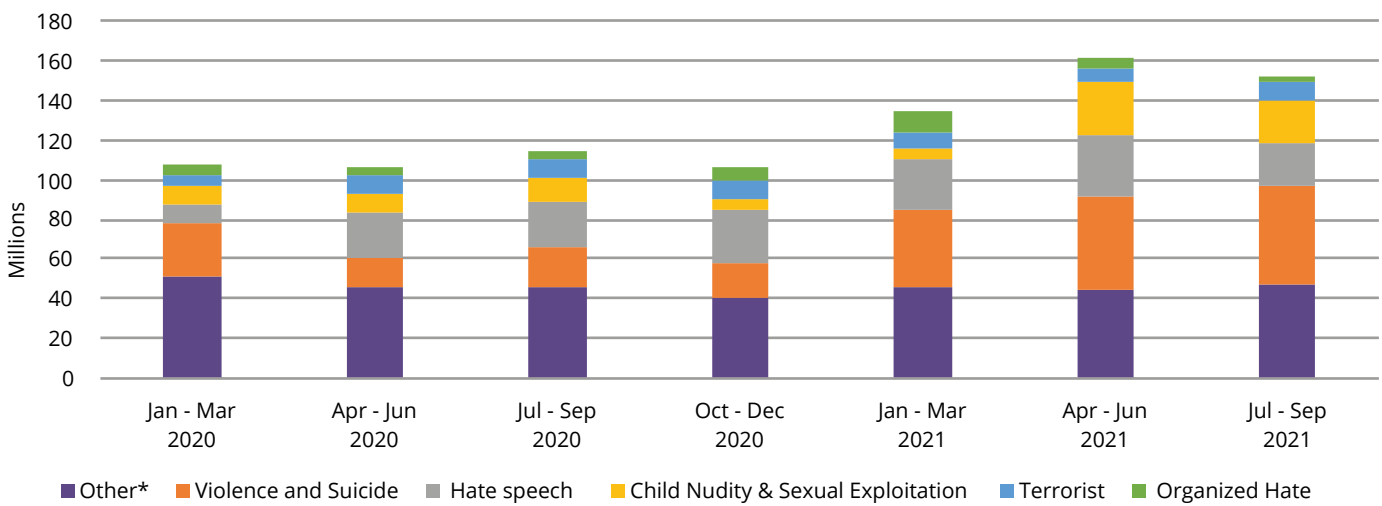
Hate speech, terrorist content and protection of minors

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 MSs such as Denmark, France and Germany, as well as the UK. 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

Fig. 1.2.3 Content removed from Facebook, by reason

Source: Facebook



**Adult Nudity & Sexual Activity, Bullying & Harassment, Drugs, Firearms*

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

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.

Data published by Facebook on hate speech content shows that, in the last quarter only, the social network acted against over 22.3 million content pieces of this kind (which become 24.3 million also considering organised hate). Fortunately, the trend is decreasing, and between the second quarter of this year and the last, hate content removed reduced by 9.2 million (-29%). In terms of numbers, the most troubling issue is related to violence and suicide which unfortunately amounted to over 48 million in the last quarter, a slight increase compared to the previous period. Another extremely worrying problem is that of the contents related to child nudity' and sexual exploitation. After an explosion in the second quarter of 2021 (+512%) data shows, fortunately, a decrease in the amount of content of this type which was intercepted. Between the second quarter of 2021 and the third, child-pornography content removed dropped from 25.6 million to about 20.9 million (-19%). The social network must also deal with a huge amount of content flagged as terrorist. According to the latest data published, in the third quarter of 2021, Facebook blocked approximately 9.8 million terrorist messages (Fig.1.2.3).

Similar issues were faced by Twitter which, in the first half of 2020, acted against 1,126,990 accounts and over 1.6 million content pieces flagged as hateful conduct (Tab.1.2.1). To understand the magnitude of the problem, these accounted for about 36% of the total content removed for violating the platform rules.

1.2.2.3. Digital advertising: EU market, consumer protection and the latest technological developments

Differently from the advertising market considered as a whole, digital advertising has experienced a continuous growth during the last 15 years with an average annual growth of about +20% from 2006 to 2019. At the same time, the Covid-19 crisis has strongly impacted digital advertising, which, in 2020, registered a minimum growth rate (+6.3%), even lower than that registered during 2008/2009 financial crisis. According to the last data available, the digital advertising market in Europe is very close to exceeding a total turnover of €70 billion (Fig.1.2.4).

According to the distinction used by IAB (Interactive Advertising Bureau) Europe, **digital advertising is made up of three main segments:**

- **search**, that includes advertising appearing on specific word requests on search engines;

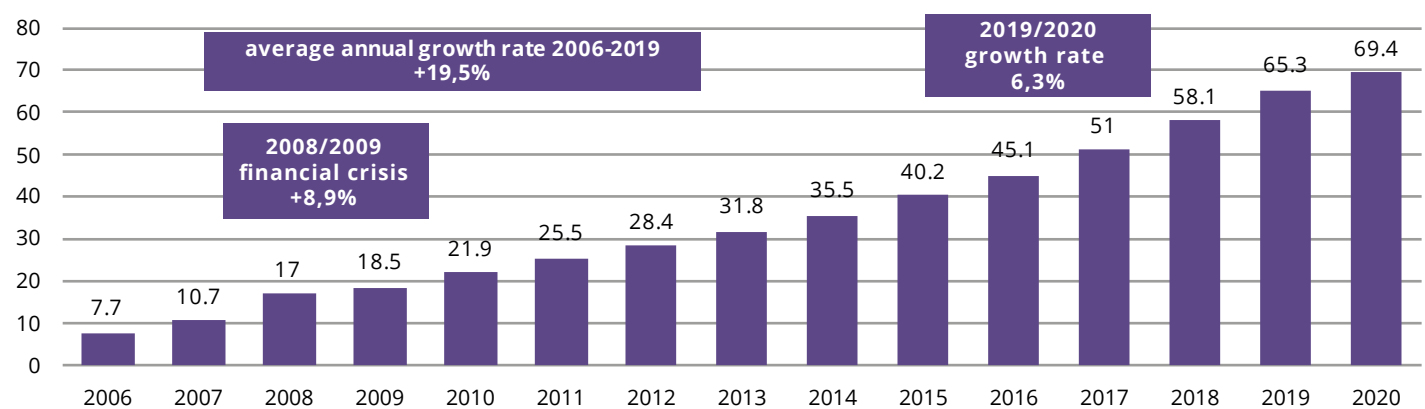
Tab. 1.2.1 Accounts suspended and content removed by Twitter (July-Dec 2021)

Source: Twitter

	Accounts actioned	Accounts suspended	Content removed
Abuse/harassment	964,459	86,202	1,448,418
Child sexual exploitation	469,439	464,804	9,178
Civic integrity	6,469	64	8,122
COVID-19 misleading information	3,399	597	3,846
Hateful conduct	1,126,990	157,615	1,628,281
Illegal or certain regulated goods or services	103,285	53,696	236,119
Impersonation	141,033	126,750	15,816
Non-consensual nudity	27,087	3,693	52,442
Private information	42,894	2,885	65,001
Promoting suicide or self-harm	188,561	4,287	226,905
Sensitive media	706,979	42,801	728,778
Terrorism/violent extremism	58,750	58,750	-
Violence	49,146	34,829	59,933
Total	**3,888,491**	**1,036,973**	**4,482,839**

Fig. 1.2.4 Digital advertising spent in Europe (€ bln)

Source: IAB - Guide to the Post Third Party Cookie Era (February 2021)



- **display**, that includes banners, buttons, skyscrapers, overlays, interstitials, pop-ups displayed on a website, as well as online video advertising.
- and **"classified[11], directories[12], affiliate[13]"**.

A further distinction made by IAB Europe is connected to *social display* vs *non-social* ads. The first involves advertising on social networks such as Facebook, LinkedIn, etc., while it is worth noting that, according to this classification, YouTube is not counted as a social network.

Looking at the numbers, while *classified, directories, affiliate* showed a 9.1% decrease in 2020, *Search* adverting rose to €30.3 billion (+7.9%). *Display* advertising reached the highest peak (€31.8 bln), increasing by 9.1%. Within the display segment, social networks showed the biggest growth (+15.9%) reaching €16.1 billion, while the *Other Display* only grew by 2.9%, up to €15.6 billion (Fig.1.2.5).

IAB also made another important distinction for display ad using programmatic distinguishing it from programmatic advertising in the traditional form[14]. The former uses automation mechanisms that rely on a set of rules applied by software and algorithms adopting different models (the most famous is related to real-time bidding, RTB)[15] that help buyers, sellers and intermediaries of advertising spaces to better allocate those spaces, giving more satisfaction both to the ad sellers, which can optimise their sales, and to the ad buyers, which can reach more interested customers and increase their return on ad spending (ROAS).

The impact of programmatic is also shown by the most recent revenue data. While traditional display ad registered a -1.6% decrease in 2020, display ad spending using programmatic saw a 7.6% increase (Fig.1.2.6). Moreover, data presented by IAB Europe in this calculation does not include social networks, the sector presenting the strongest growth[16].

Programmatic advertising has several advantages, such as allowing advertising performance to be measured and adjusted in real-time as campaigns evolve and, above all, aggregating different media properties. The advertising supply aggregation, in particular, has the effect of lowering barriers to market participation for smaller publishers trying to sell their advertising space. Indeed, smaller publishers can compete for advertising money that alone they would not be able to reach, since

11 The fee is paid by an advertiser to display an ad or listing regardless of the outcome of the ad (i.e., even if there is no 'sale').

12 Online directories online version of printed "yellow pages".

13 Fees paid to third parties (affiliates) for traffic generation (e.g., pay-per-visit).

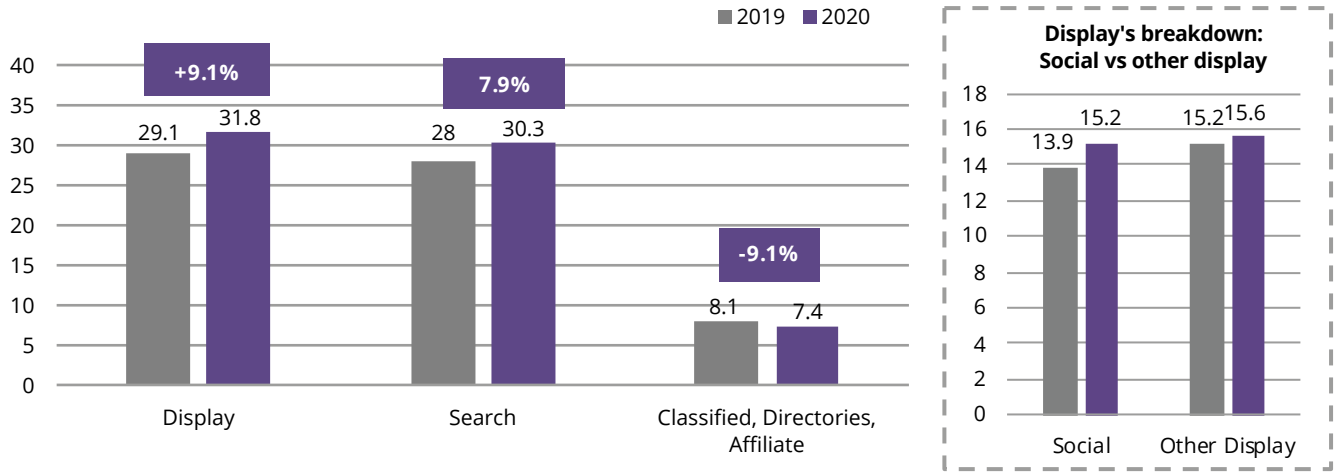
14 Following the IAB's proposed taxonomy, 'programmatic' is considered as an aggregate category made up of four different transactional models: Automated Guaranteed, Unreserved Fixed Rate, Invitation-Only Auction, Open Auction. Hence, the advertising revenues are considered as 'programmatic' whenever any of those mechanisms applies. Revenue is considered programmatic even if inventory that is originally sold to an intermediary through non-programmatic means (e.g. agency bulk buying) is re-sold to an end-buyer programmatically.
Source: IAB Europe, AdEx Benchmark report.

15 Real-time bidding (RTB) is one of the programmatic subsets. It implies that the price to determine the appropriate price of a unit of ad inventory is made through real-time auctions (in which, generally speaking, each user had pre-set the maximum they are willing to bid).

16 As specified by IAB, some markets define programmatic as including social, others as excluding social. In this data presentation, they use programmatic excl. social in order to better document the market dynamics of the so-called 'open internet'. Data, which includes banner, video and audio, has been harmonised between markets based on IAB Europe calculations.

Fig. 1.2.5 Digital advertising spent in Europe, by segment (€ bln)

Source: IAB - Guide to the Post Third Party Cookie Era (February 2021)



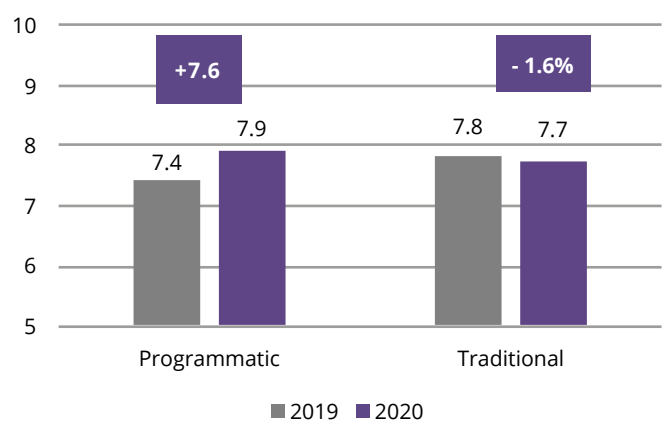
they are too small to be known and lack the networking and sales force which large media companies have.

These complex technological mechanisms and, consequently, the impressive growth of digital advertising, rely at most on data usage. This data, on the one hand, fuels the workflow automation mechanisms of programmatic advertising and, on the other hand, addresses consumers who are potentially more interested in advertised products and services, because of their preferences, previous experiences or other circumstances (targeted advertising).

In this way, **behavioural data**, which includes both on-site and off-site browsing, allows companies to tailor more specific advertising messages and to choose the most relevant place or moment to convey

Fig. 1.2.6 Spent in display advertising, by type (€ bln)

Source: IAB - Guide to the Post Third Party Cookie Era (February 2021)



them. Indeed, as modern trends push people's tastes and cultural affiliations to diversification, the traditional criteria for segmenting consumers (such as age, income, etc.) have become insufficient. To fill this gap, behavioural data allows advertisers to better identify the potentially interested user, reducing the percentage of messages delivered to uninterested customer, so decreasing customer frustration, as well as the marketing campaign costs for the advertisers, and maximising satisfaction.

For these reasons, **limiting the use of consumer data can be particularly damaging for the advertising industry, without bringing any concrete advantages or further protection for consumers.**

In 2016, 90% of the digital display advertising market growth came from formats and processes that used behavioural data. Assuming that this trend remained unchanged (while it probably moved even more toward behavioural data analysis), **this would mean that, on the total display advertising market (equal to €31.8 billion in 2020), about €28.6 billion would be directly impacted by a limitation on behavioural data collection.**

This is due to the fact that behaviourally targeted ads have a much higher click-through rate (percentage of customers who click on the ad) compared to the standard advertising without behavioural data. According to IHS Markit, on average this is 5.3x higher, and up to 10.8x higher when data is used to retarget people who have previously looked at a product. For advertisers, which are now accustomed to this kind of result, behavioural targeting has become a prerequisite for spending their advertising budget on digital media channels.

In 2017, IHS Markit suggested that blocking behavioural advertising would mean a market decrease between of 30% and 50% of this segment[17], which would account for about between €8 billion and €14 billion in losses per year. Even more importantly, this decrease would affect small players much more seriously (from 50% to 70% reduction) than market participants with large-scale 1st party data (up to a 10% decrease)[18].

Recommendation systems

Another technology closely connected to data usage is that of *recommendation systems*, tools used to provide users advertising based on their preferences.

Thanks to the recommendation systems the seller can personalise the user experience by delivering accurate, customised recommendations of products to users according to their preferences.

Many different methodologies and concepts of recommendation systems make them suitable for various applications including e-commerce, healthcare, transportation, agriculture and media.

At the same time, **recommendation systems are based**

17 This is a conservative estimate elaborated with 2017 values. The percentage of ad spending using behavioral data has probably increased in 2020.

18 According to the IHS Markit estimates, publishers who are not in the top 50% of market size players would, on average, see revenue contractions between 2x and 5x more pronounced than larger counterparts. Publishers whose content and audiences are available through other publishers and sites would see revenue contractions 3x to 5.5x more pronounced than those whose content or audience scale makes them indispensable for advertisers.

on the categories of collaborative filtering, content-based, utility-based, demographic-based, knowledge-based and hybrid-based.

The most popular filtering approaches use content-based and collaborative filtering. Collaborative filtering works by developing a database of the user's preferences for products. If a collaborative filtering system is active, users are registered on this database to discover individuals with similar purchase preferences. The content-based approach crosses the content of an element and the profile of a user. The content of an element includes its description, attributes, keywords and tags. This data is compared with the preferences identified by analysing the elements viewed by a user while browsing. By comparing the content of the elements and the profile of preferences, the recommendation engine suggests the user the products that are closest to his/her interests.

Demographic recommendation systems generate ads by categorising users on demographic attributes – an approach especially useful when product information is limited. The advantage of demographic filtering is that it is fast and allows for obtaining results using only a few observations. However, demographic-based filtering techniques have several disadvantages. For example, they do not acquire the user ratings essential for content-based and collaborative-based filtering techniques.

Utility-based recommendation systems provide ads based on generating a utility model of each item for the user. This system recommends highest utility item based on each item's calculated user-utility. Utility-based systems can factor attributes not related to the product into utility functions, such as product availability and vendor reliability. So, utility systems are not based on long-term generalisations on user preferences and behaviour. Instead, they evaluate a recommendation based on the user's current needs and the available options.

Knowledge-based recommendation systems use knowledge about products and users to create a criterion to generate ads. This system does not require an initial large amount of data because its recommendations are independent of the user's ratings. The knowledge-based system then associates products with characteristics that most closely resemble user preferences.

Hybrid recommendation systems combine two or more techniques to obtain better performance. Their main target of this approach is to eliminate the weaknesses of the individual technique. For example, some video and music steaming platforms, to recommend products to the user, use both similar user ratings and the content of the cross-element to the user's profile.

Recommendation systems are extremely useful but can face various challenges. This term comes from the mobility world and refers to the difficulty of starting a cold engine. Also, recommendation systems with insufficient information or metadata available can suffer from this problem. Specifically, almost all new products posted on an e-commerce site go through the product cold start because there are no reviews due to the lack of user interaction. Another problem that recommendation systems often run into is related to data sparsity. This results from the fact that the users do not always rank

items because of the lack of incentives or knowledge to rate them. As the number of users grows, many e-commerce sites that use recommendation systems also face scalability problems. This happens because new methodologies need to generate quick results for large scale applications.

Algorithms experience performance issues for consumers with large amounts of information. For a platform that reaches millions of users and products, scalability is a serious issue. A useful technique to reduce scalability issues is by using clustering. This technique involves segmenting the users using a clustering algorithm, and uses each element as a group. Recommendation systems may provide the most accurate results by recommending items based on user or object similarity. This is known as the diversity issue, where recommendations are based on overlapping, instead of differences. In fact, the system exposes the user to a narrower selection of objects, while highly related niche items may be overlooked.

The last of the most important problems of the recommendation system is related to habituation effect. Customers are overwhelmed by too much information, especially marketing content. This situation leads to a habituation effect which ends in banner blindness. Recommendations that are optimal from the algorithmic perspective may provide inaccurate results if badly visualised by the user. To avoid banner blindness, marketers usually use techniques based on increasing the visual intensity of presented objects with the use of animations and flickering effects.

Consumer protection: opt-in, third party cookies and anonymisation strategies

Over the last years, European and national institutions have become increasingly aware of consumer privacy and data protection. This is due to the trend taking place in online data collection, where millions of customers have been providing (sometimes very private) data often without a real and concrete awareness of the consequences of their actions.

At the same time, setting aside situations where data has been collected improperly and maliciously – which is clearly a crime to be stopped and persecuted -, it is worth noting that, as described in the previous paragraph, data collection is extremely effective in optimising advertising campaigns and is often necessary to allow basic web functions to work (see functional cookies[19]).

Moreover, recent legislation, in particular, the ePrivacy Directive and the GDPR provisions on cookies, does not seem to have provided any real improvement in terms of user friendliness (and, sometimes, also for consumer protection). After a first phase, which saw the introduction of new pop-ups asking for a "yes" from the consumer in order to proceed, the current situation has evolved into a plethora of different interfaces which ask

19 According to the IAB Europe definition, a cookie is a name (=key), a value (some data, e.g. ID for advertising or other) and attributes (e.g. domain, path, expiry date, size, HTTP only, secure and same site). Cookies can be first party or third party, according to the fact that the user is on the first party website or moves to other websites, which gives to the former or next (third parties) indications about its movements. The cookie is not an identifier in itself, even if it can hold data.

for multiple permissions that most of the time confuse the customers, who tend to accept all the conditions without really understanding what they are clicking on.

In addition, in the "technicalities" war between legislation and technology, it is worth remembering that the latter can always make the first move. Currently, the strategy of reducing cookies usage is producing the side effect of encouraging opaque tracking techniques, such as fingerprinting. By using very small bits of information that differ between users, these techniques can generate unique identifiers to follow the users in their web surfing without cookies. Moreover, unlike cookies, this data cannot be deleted, so the users could, paradoxically, have less control over their privacy than before.

In order to face these issues, the advertising industry is experimenting with different solutions. In 2019, Google announced it would progressively remove third party cookies from its Chrome browser, which will definitely stop working by 2022. In this way, Google joins the other two main browser providers – Mozilla (Firefox browser stopped using third party cookies between January and September 2019) and Apple (Safari browser has not allowed third party cookies since June 2017). The main goal of this operation is to create a *privacy sandbox* to protect anonymity while still delivering results to advertisers (and consequently, revenues to publishers). Google is currently experimenting with anonymisation techniques in order to provide probabilistic data coming from groups of consumers similar habitudes, in order to provide advertisers with meaningful behavioural data while guarantying full user anonymisation[20].

Different projects are currently looking for innovative solutions in order to find alternatives to cookies. Amongst these, there is the W3C and IAB Tech Lab's Project Rearc. The World Wide Web Consortium (W3C) is an international community that develops open technical specifications and standards to ensure the long-term growth of the web, while the Rearc project tries to balance consumer privacy and personalisation and is working on developing new technical standards and guidelines driving "privacy by default" addressable advertising and measurement.

As well, involving telco providers could be a potential solution. The real time nature of a telco network enables the use of a Telco Verified User ID and a Dynamic ID for audience transactions at an individual per ad request level. In this case, the telco operator would provide a single identifier for each user – who would remain unknown to advertisers – allowing the latter to profile these "identifiers" and fine tune their marketing strategies according to tastes and behaviour.

Indeed, it is important to note that user addressability in digital advertising does not aim to identify an individual person by name, address or phone number but, rather, to generate a persistent pseudonym to engage and optimise against when buying media or delivering ads[21]. Hence, the key concept is to identify the best solution

20 See Evaluation of Cohort Algorithms for the FLoC API https://github.com/google/ads-privacy/blob/master/proposals/FLoC/FLOC-Whitepaper-Google.pdf

21 See IAB Europe, Updated Guide to the Post Third-Party Cooke Era, February-2021, pp. 31

to anonymise customers, in terms of preserving their identity, while still keeping their characteristic and behavioural data available for advertisers and publishers. Since technology seems to be capable of reaching this goal, this way appears to be much more effective than simply blocking or complicating the tracking, also because this provision leads to the undesired side effects described above (ad industry revenues fall, publisher crisis, search for alternative ways, legally or illegally, of customer profiling). For these reasons, it seems desirable that new legislation should take into account this technological evolution and find a way to support and provide incentives to spread innovative forms of privacy protection with the use of anonymisation technologies.

1.3. DATA REGULATION

1.3.1. The data economy in the EU and the enabling technologies

The Internet of Things, social media, mobile applications, and other new technologies are generating an unprecedented amount of data. According to some estimates, the total amount of data created, captured, copied, and consumed globally was forecasted to increase rapidly, reaching 64.2 zettabytes in 2020. Then over the next five years, up to 2025, global data creation is projected to grow to more than 180 zettabytes (Fig. 1.3.1).

Nowadays, most economic activity depends on the sharing of and the use of data, and in the future this trend will continue to increase with a huge economic

Fig. 1.3.2 Data economy impact on the EU-27 GDP

Source: IDC European Data Market Monitoring Tool (2020)

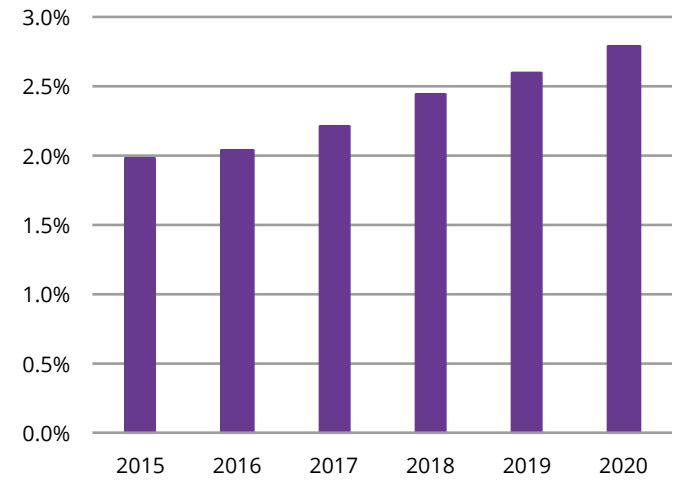
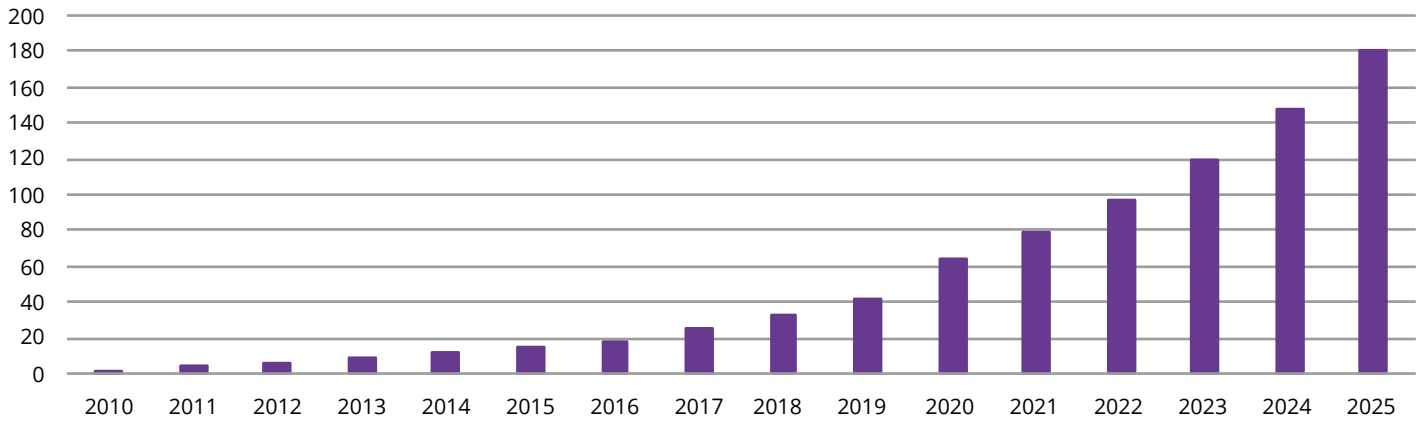


Fig. 1.3.1 Volume of data/information created, captured, copied, and consumed worldwide (in zettabytes)

Source: Statista (2021)



impact. According to the IDC European Data Market Monitoring Tool (2020), the value of the data economy – which measures the overall impact of the data market on the economy as a whole – exceeded the threshold of €300 billion in 2020 for the EU-27. In relative terms, the impact of the data economy on the EU-27 GDP is 2.8%, up by 0.8 percentage points compared to 2015 (Fig. 1.3.2). Therefore, the impact of the data market on the EU economies is becoming more significant, ranging from 1% in Greece to 4.9% in Estonia in 2020 (Fig. 1.3.3).

Fig. 1.3.3 Data economy impact on GDP, by country

Source: IDC European Data Market Monitoring Tool (2020)

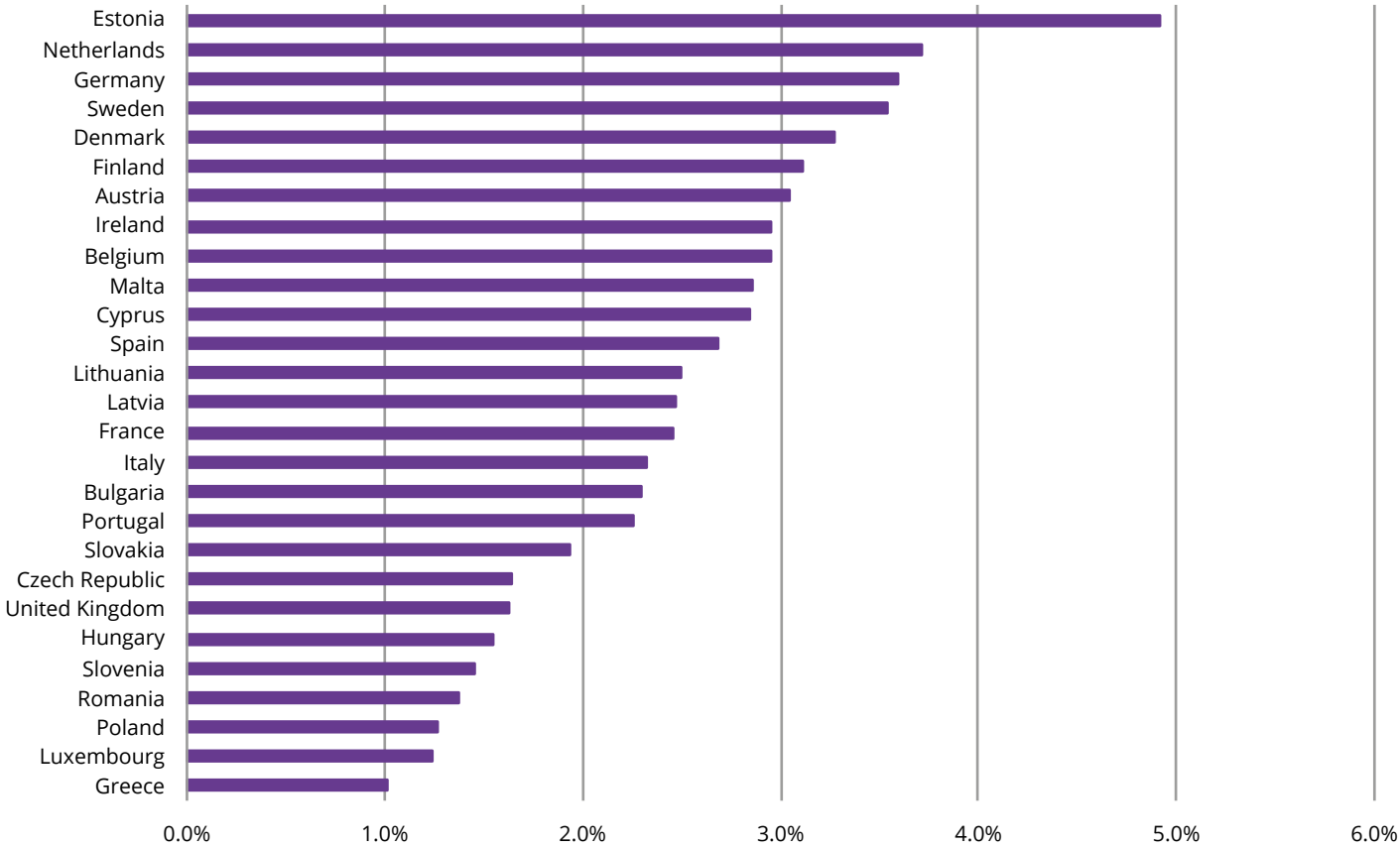
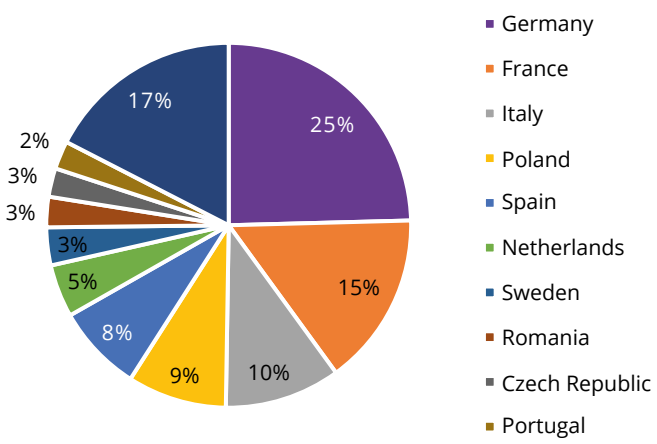


Fig. 1.3.4 Distribution of data professionals across EU-27 (2020)

Source: IDC European Data Market Monitoring Tool



Finding value in data is about analysing it, and this requires insightful data professionals and enabling technologies such as big data analytics, artificial intelligence and cloud computing.

In 2020, there were more than 6.6 million data professionals in the EU, with 50% concentrated in three Member States – Germany, France and Italy (Fig. 1.3.4).

However, where enabling technologies are concerned, only 13% of European companies make use of BDA tools. The best performing countries are Malta and the Netherlands where 29% and 26%, respectively, of company use such tools (Fig. 1.3.5).

Regarding the **uptake of AI technologies in the EU** (Fig. 1.3.6), Eurostat data shows that the adoption of least one AI technology is highest in Ireland (20%), followed by Malta (37%) and Finland (10%). The uptake of one

Fig. 1.3.5 Enterprises analysing big data internally from any data source (%, 2020)

Source: Eurostat

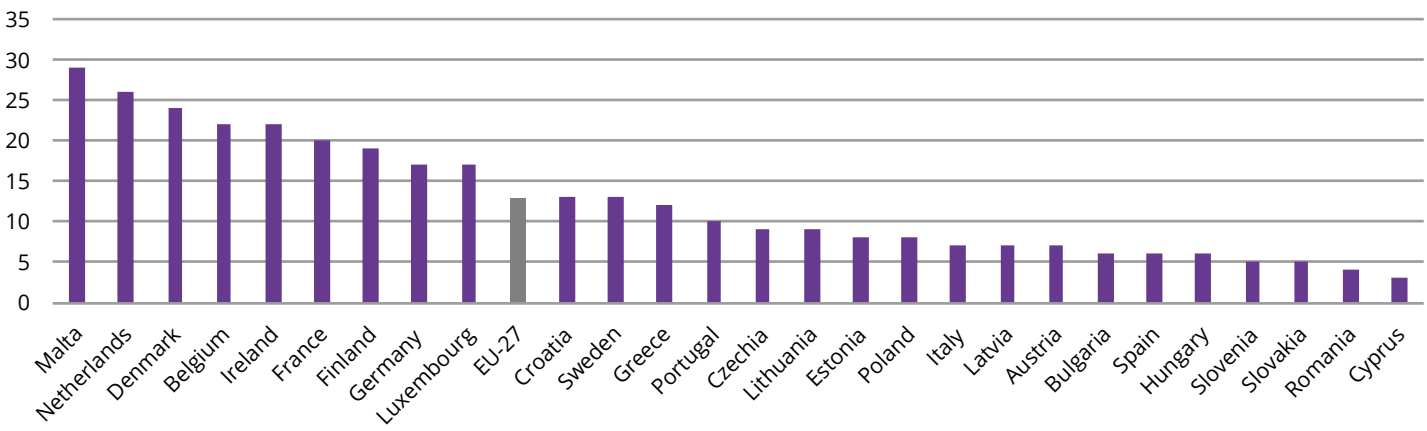


Fig. 1.3.6 Enterprises using one AI system (%, 2020)

Source: Eurostat

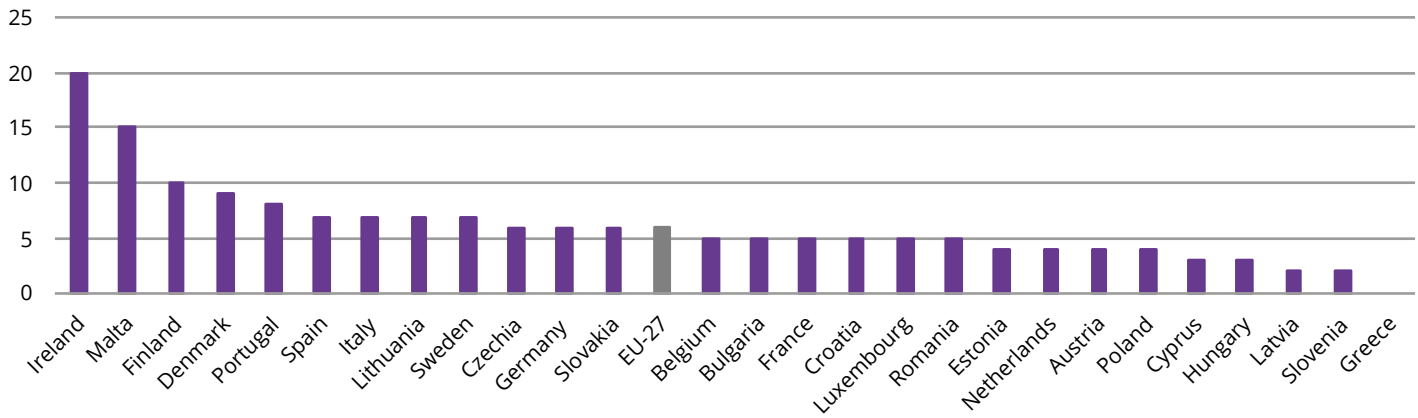
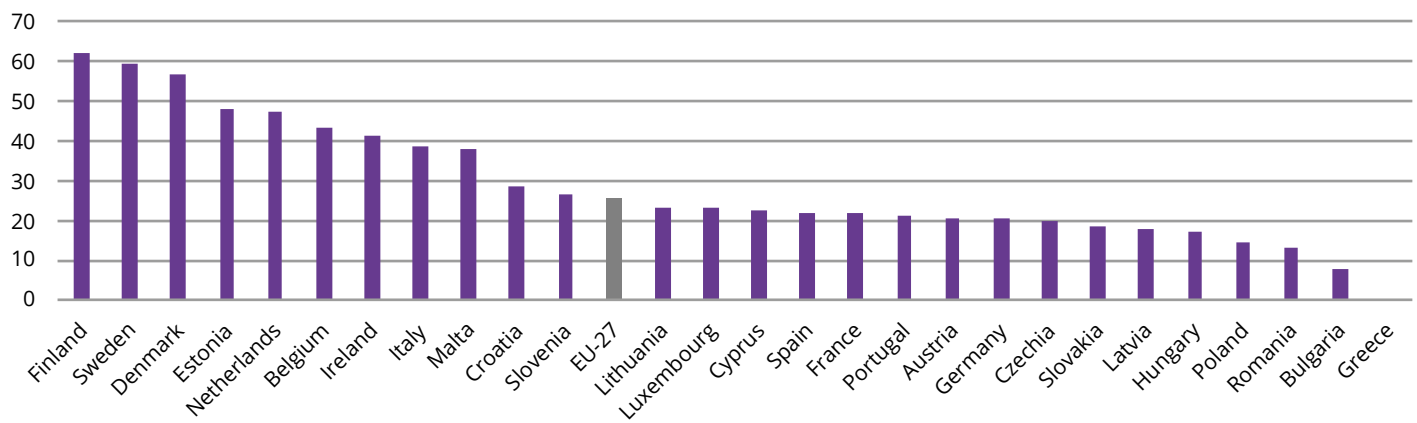


Fig. 1.3.7 Enterprises buying cloud computing services of medium-high sophistication (%, 2020)

Source: EU Commission



AI technology is lower in Slovenia, Latvia, Hungary and Cyprus. The EU average is only 6%.

In 2020, 26% of EU enterprises purchased cloud computing services of medium-high sophistication. Nordic enterprises are leaders in incorporating cloud services of medium-high sophistication, with more than 60% of Finnish enterprises buying such services, followed by Sweden and Denmark at more than 55%. However, the gap between top and low performers remains large, with Bulgaria scoring below 10% (Fig. 1.3.7)[22].

1.3.2. Data regulation: from the GDPR to the Data Act. The European regulatory framework on data usage and protection

The digital revolution finds its lifeblood in data. The attention of European institutions has for years been focused on two different aspects – the **protection of personal data** and the **creation of an ecosystem enabling data circulation and use**.

In the first stages, European institutions defined a regulatory framework based on Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, Regulation (EC) No 45/2001 on the protection of individuals for the processing of personal data by the Community institutions and bodies and on the free movement of such data, and Directive 2002/58/EC **– E-Privacy Directive. These** were the first initiatives to ensure a set of rules able to guarantee the protection of personal data in the EU.

However, the most important initiative, which has enabled the EU to become a model at global level, is the adoption, in April 2016, of **Regulation n. 2016/679** on the protection of individuals for the processing of personal data and on the free movement of such data. This is a very important regulatory intervention that has laid down the foundations of lawfulness of data processing, indicated in an exhaustive manner the timing, contents and modalities of the information notice, defined the rights of data subjects (access, cancellation-oblivion, limitation of processing, objection, portability), identified the subjective characteristics and responsibilities of data controllers and data processors (introducing, among the various criteria, that of 'data protection by default and by design' and of risk) and regulated international data transfers. One of the most relevant aspects concerns the territorial scope. In fact it applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not and to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

22 https://digital-strategy.ec.europa.eu/en/policies/desi

Successively, on 23 October 2018, the **Regulation n. 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) n. 45/2001 and Decision n. 1247/2002/EC** was adopted. It lays down rules on how EU institutions, bodies, offices and agencies should treat the personal data they hold on individuals, upholds an individual's fundamental rights and freedom, especially the right to protection of personal data and the right to privacy and aligns the rules for EU institutions, bodies, offices and agencies with those of the General Data Protection Regulation (GDPR) and of Directive (EU) 2016/680.

From the analysis of the technological developments (especially new Internet-based interpersonal communication services or new IoT technologies), on 10 January 2017, the European Commission launched a proposal for a **regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).** In detail, the proposal, which is the subject of a complex adoption procedure that has not yet been finalised, aims to ensure a higher level of privacy protection for users of electronic communications services, consistent with the GDPR and the state of the art. It lays down rules on the protection of fundamental rights and freedoms of natural and legal persons with regard to the provision and use of electronic communications services, primarily the right to privacy and communications, and the protection of individuals with regard to the processing of personal data. This proposal, in particular, starting from the consideration that electronic communications data shall be confidential, identifies permitted processing of electronic communications data, regulates storage and erasure of electronic communications data and consent (in line with GDPR), prescribes information and options for privacy setting, sets specific rules on incoming call blocking, publicly available directories and unsolicited communications fixing information obligations on providers specifically with regard to the consent of end-users.

Alongside the need to ensure effective protection of personal data, the intention of the institutions to ensure that individuals, businesses and public administrations can benefit from the enormous opportunities associated with the use of data is also a priority. In fact, considering that digital technologies have transformed the economy and society, affecting all sectors of activity and the daily lives of all Europeans and that data is at the heart of this transformation, on 14 November 2018, **Regulation n. 2018/1807 on a framework for the free flow of non-personal data in the European Union** was adopted. It aims at ensuring the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users. To this end, the regulation encourages the development of self-regulatory codes of conduct at Union level in order to contribute to a

competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards (to be developed in close cooperation with all relevant stakeholders, including associations of SMEs and start-ups, users and cloud service providers) and prescribes MSs to designate a single point of contact regarding the application of this regulation.

Successively, focusing on the public sector, the European institutions adopted **Directive n. 2019/1024 on open data and the re-use of public sector information (Open Data Directive)** which sets timelines, procedures to process the request for re-use and the conditions for re-use identifying available formats and principles governing charging and conditions (specific rules are set for high-value datasets). The same directive encourages MSs to make practical arrangements facilitating the search for documents available for re-use, such as asset lists of main documents with relevant metadata, accessible where possible and appropriate online and in machine readable format and portal sites that are linked to the asset lists, and support the availability of research data by adopting national policies and relevant actions aiming at making publicly funded research data openly available.

In February 2020, instead, the Communication "***A European Strategy for Data***" outlined the European strategy consisting of a series of measures and investments to enable the data economy over the next five years. This communication presents a European data strategy aimed at making the EU the most attractive, secure and dynamic data-agile economy in the world – empowering Europe with data to improve decisions and better the lives of all of its citizens. To achieve this goal, the document identifies several critical issues that need to be overcome concerning the availability of data, imbalances in market power, data interoperability and quality, data governance, data infrastructures and technologies, empowering individuals to exercise their rights, skills and data literacy and cybersecurity. Considering these issues, the Commission has outlined a strategy focused on four pillars and several key actions to encourage a cross-sectoral governance framework for data access and use, to strengthen Europe's capabilities and infrastructures for hosting, processing and using data, interoperability to reinforce competences and skills and to create common European data spaces in strategic sectors and domains of public interest (specifically, manufacturing, Green Deal, mobility, health, finance, energy, agriculture, public administrations and skills).

Implementing the strategy, on 25 November 2020, the Commission proposed a regulation on European data governance (**Data Governance Act**) which aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. The proposal, complementing the Directive n. 2019/1024 of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive), includes measures to: 1) increase trust in data sharing, as the lack of trust is currently a major obstacle and results in high costs; 2) create new EU rules on neutrality to allow novel data intermediaries to function as trustworthy organisers of

data sharing; 3) facilitate the reuse of certain data held by the public sector; 4) give Europeans control over the use of the data they generate, by making it easier and safer for companies and individuals to voluntarily make their data available for the wider common good under clear conditions.

The regulation lays down conditions for the re-use, within the Union, of certain categories of data held by public sector bodies (specifically, data held by public sector bodies which are protected on grounds of commercial confidentiality, statistical confidentiality, protection of intellectual property rights of third parties and protection of personal data), identifies specific data sharing services subject to notification procedure to the competent authority (which may charge fees) and identifies the information to be included, regulates data altruism and general requirements for registration of data altruism organisations, identifies requirements relating to competent authorities and sets the right to an effective judicial remedy, allows the Commission to establish a European Data Innovation Board in the form of an Expert Group, made up of representatives from competent authorities of all the Member States, the European Data Protection Board, the Commission, relevant data spaces and other representatives of competent authorities in specific sectors and identifies the tasks.

More dedicated proposals on data spaces are expected to follow in 2022, complemented by a Data Act to foster data sharing among businesses, and between businesses and governments.

1.3.3. The European digital sovereignty and the role of enabling technologies: the main European initiatives on cloud

The growing importance of digital technology has made the debate on the digital sovereignty of the European Union more and more central. First of all, the specific definition of "digital sovereignty" can vary according to the contexts in which the expression is used and the kind of self-determination – state, corporate or individual – that is emphasised. In fact, if the focus is on state or regional autonomy, digital sovereignty could be defined as control over digital infrastructures. Conversely, if the focus is on corporate domains, digital sovereignty could mean economic autonomy, i.e. the autonomy of the national economy from foreign technologies and services. Finally, individual autonomy yields a definition of digital sovereignty as self-determination of the citizen in his or her roles as employee, consumer and user of digital services or technologies.

Cloud services, in particular, are very relevant digital infrastructures that the European Commission considers critical in consideration that the most important cloud service providers are non-EU companies. For this reason, the Commission is especially concerned about the issues regarding data ownership and management within European MSs and on the potential lack of privacy and absence of data protection for personal information collected by foreign providers.

In the European strategy for data just analysed, the Commission announced for the period 2021-2027,

investments in a High Impact Project on European data spaces and federated cloud infrastructures. The project will fund infrastructures, data-sharing tools, architectures and governance mechanisms for thriving data-sharing and AI ecosystems. It will be based on the European federation (i.e. interconnection) of energy-efficient and trustworthy edge and cloud infrastructures (Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-aService services).

Specifically, the Commission intends to fund the establishment of EU-wide common, interoperable **data spaces in strategic sectors** that are manufacturing, the Green Deal, mobility, health, financial, energy, agriculture, skills, and for public administration data spaces. Such spaces aim at overcoming legal and technical barriers to data sharing across organisations, by combining the necessary tools and infrastructures and addressing issues of trust. The spaces will include the deployment of data-sharing tools and platforms, the creation of data governance frameworks and improving the availability, quality and interoperability of data – both in domain-specific settings and across sectors. Funding will also support authorities in the MSs in making high value data sets available for reuse in the different common data spaces. The support for data spaces will also cover data processing and computing capacities that comply with essential requirements in terms of environmental performance, security, data protection, interoperability and scalability.

In this context, the Commission will foster synergies between the work on European cloud federation and MS initiatives such as the "Gaia-X" cloud project, a federated data infrastructure to enable the management, access and control of data belonging to EU citizens and businesses. The aim of the initiative, launched by France and Germany, is to ensure interoperability and security standards in order to promote an open and transparent digital ecosystem, where data and services can be made available, collected and shared in a secure environment, rather than to create a European cloud alternative to US and Asian providers. The project envisages the creation of a new pan-European platform that brings together different cloud service providers, including non-European, as long as they accept the set of requirements, standards and values promoted at EU level, first of all data sovereignty for users.

Amongst the goals indicated in the strategy, the Commission announced the launch of a European cloud services marketplace, integrating the full stack of cloud service offering (Q4 2022) and the creation of an EU (self-)regulatory cloud rulebook (Q2 2022).

In addition to the commitment to establishing the European federal cloud within the framework of the Gaia X project, on December 2020, the European Commission launched a **European Alliance on Industrial Data, Edge and Cloud**, made up of representatives of the MSs, cloud computing providers and industrial cloud users. It will feature the development of several work streams, related to key EU policy goals: 1) joint investment in cross-border cloud infrastructures and services to build the next generation cloud supply, including to enable Common European Data Spaces; 2)

EU Cloud Rulebook for cloud services, which will provide a single European framework of rules, transparency on their compliance and best practices for cloud use in Europe; 3) a European marketplace for cloud services, where users will have a single portal to cloud services meeting key EU standards and rules. It is expected to lead the implementation of the pan-European cloud with a budget of up to €10 billion.

1.4. A EUROPEAN LEADERSHIP ON TRUSTWORTHY ARTIFICIAL INTELLIGENCE

1.4.1. The potential of artificial intelligence for our society

The benefits deriving from **artificial intelligence (AI)** concern the industrial world but also affect society as a whole. Companies are increasingly using AI as a new factor for industrial growth and as a lever for competitiveness and to achieve benefits in terms of greater reliability, greater quality and safety, lower operating costs and higher revenues and profits. AI technology helps companies raise the quality of human work, to free up workers from repetitive, onerous and dangerous tasks, to increase turnover and profits and to acquire new customers, as well as to limit risks and improve efficiency in general. Consider, for example, the real-time identification of fraudulent transactions or predictive maintenance in the manufacturing sector or even faster and more reliable delivery of consumer goods by a service company. However, AI is not only used to optimise the contribution of human work, but also to amplify human intelligence, providing contextual knowledge from data that the human mind alone could not access and / or process.

In the European Parliament study, "Opportunities of Artificial Intelligence"[23], we read that AI will lead to a strong increase in labor productivity (between 11% and 37% by 2035) due to innovative technologies enabling more efficient workforce-related time management.

Instead, for citizens, AI could mean better healthcare, safer cars and other transport systems, and also tailor-made, cheaper and longer-lasting products and services. It can also facilitate access to information, education and training. Furthermore, AI used in public services can reduce costs and offer new possibilities in public transport, education, energy and waste management and could also improve the sustainability of products[24]. Therefore, **AI could contribute to achieving the European Green Deal goals and UN Sustainable Development Goals.** For instance, concerning climate action, an analysis by PwC and Microsoft found that the use of AI for environmental applications has the potential to reduce global greenhouse gas emissions by between 1.5% and 4% by 2030[25]. Moreover, **AI and machine learning have the capabilities to address also major health challenges**, such as the current pandemic. AI technologies and tools have played a key role in every aspect of the Covid-19 crisis response from prediction and tracking of the spread of the virus to diagnosis and development of therapies and vaccines and in the improvement of healthcare systems. In general, AI systems have the great potential to accelerate the lead times for the development of vaccines and drugs. Therefore, many life science companies have resorted to AI for drug discovery. Finally, among the various areas in which AI brings benefits, we must also mention **security**

23 European Parliament, Opportunities of Artificial Intelligence, 2020

24 https://www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities

25 European Parliament, Opportunities of Artificial Intelligence, 2020

and cybersecurity. AI is predicted to be used more in crime prevention and the criminal justice system, as massive data sets could be processed faster, prisoner flight risks assessed more accurately, and crime or even terrorist attacks predicted and prevented. It is already used by online platforms to detect and react to unlawful and inappropriate online behaviour[26]. However, AI applications also give rise to significant ethical, trust and legal challenges. These include the security, robustness and resilience of AI system privacy and data protection; transparency and accountability of AI systems; fairness, discrimination and explainability of AI systems; and liability issues. Therefore, the European commission is trying to define a clear legal framework on AI that tries to give answers to all the complex issues related to this new technology.

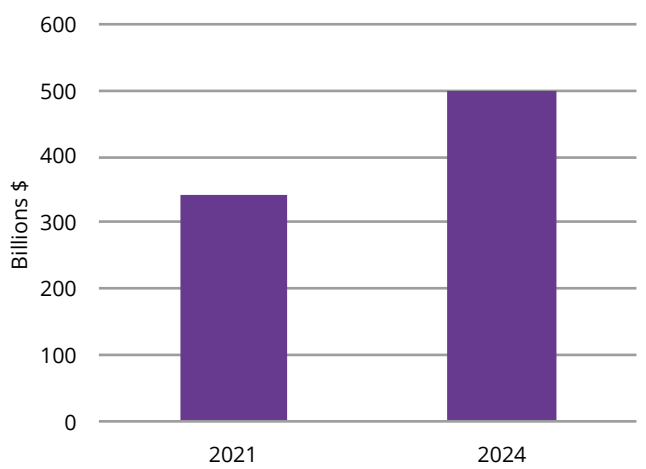
1.4.2. The global artificial intelligence market

The interest in these new technologies is confirmed by the exponential growth registered by the AI market in recent years. According to the latest release of IDC (International Data Corporation)[27], worldwide revenues for the AI market, including software, hardware and services, is estimated to grow 15.2% year over year in 2021 to $341.8 billion. The market is forecasted to accelerate further in 2022 with an 18.8% growth and remain on track to break the $500 billion mark by 2024 (Fig. 1.4.1). Of the three technology categories, **AI Software** occupied 88% of the overall AI market. However, in terms of growth, **AI Hardware** is estimated to grow the fastest in the next years. From 2023 onwards, **AI Services** is forecasted to become the fastest growing category.

Businesses and organisations across all industries are increasing their investments in AI to create a competitive advantage through improved customer insight, greater employee efficiency, and accelerated innovation. Retail and Banking are the two industries that will spend the most on AI solutions over the five-year forecast period, 47.8% and 13.8%, respectively, of total AI investment. Retail AI spending will largely focus on solutions that improve the customer experience through automated

Fig. 1.4.1 Worldwide revenues for the AI market

Source: IDC (2021)



26 https://www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities

27 https://www.idc.com/getdoc.jsp?containerId=prUS48127321#:~:text=NEEDHAM%2C%20Mass.%2C%20August%204,Corporation%20(IDC)%20Worldwide%20Semiannual%20Artificial

Fig. 1.4.2 Global AI spending, by industry (in %)

Source: IDC (2021)

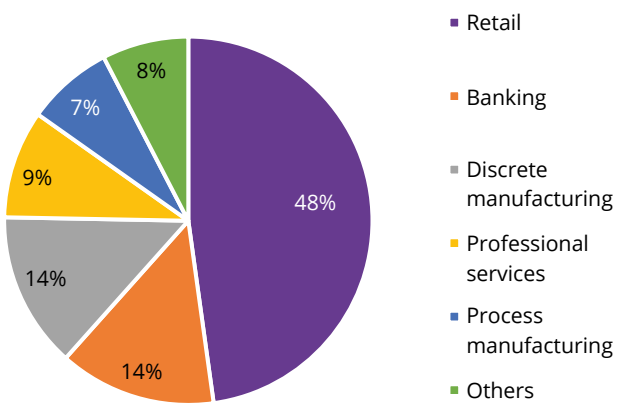
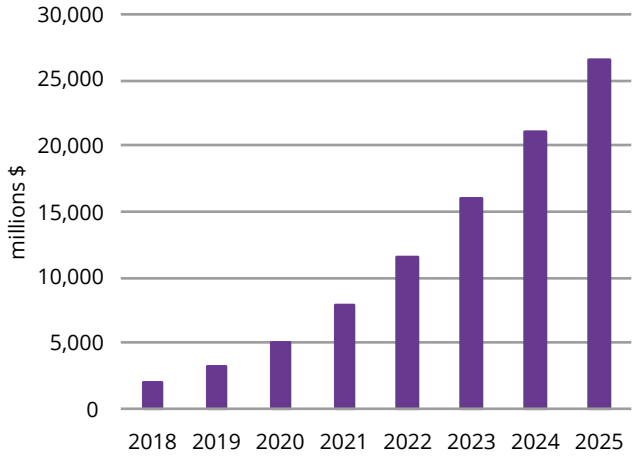


Fig. 1.4.3 Revenues from the AI software market in Europe from 2018 to 2025

Source: Statista (2021)



customer service and recommendation engines. The Banking industry will allocate much of its AI investment to risk reduction through automated threat intelligence and fraud analysis applications. The third largest industry for AI spending, Discrete Manufacturing (13.7%), will primarily invest in quality management and automated preventative maintenance solutions (Fig. 1.4.2)[28].

Interest in AI is also very strong in Europe. In fact, the European AI software market is expected to experience a significant growth in the coming years, with revenues increasing from around $2.09 billion in 2018 to an expected $26.5 billion by 2025[29](Fig. 1.4.3).

1.4.3. The EU in the global race for AI

The global race for AI sees three main players – the US, China and the EU. Each has shown a different approach to the development, implementation and regulation of AI, outlined in their respective strategies. China's strategy is mainly focused on the role of the state, which protects and invests in those businesses that have made it to the top after an initial phase of fierce domestic competition. On the other hand, the US gives a much more prominent role to the market and the investments made by big corporations, maximising space for innovation through lighter public regulation. The US strategy relies to a greater extent on voluntary self-regulation, and the protection of values that they consider as "core", such as freedom, human rights or the rule of law. Finally, the

28 https://www.idc.com/getdoc.jsp?containerId=prUS48191221
29 https://www.statista.com/statistics/1078459/europe-artificial-intelligence-market-revenues/

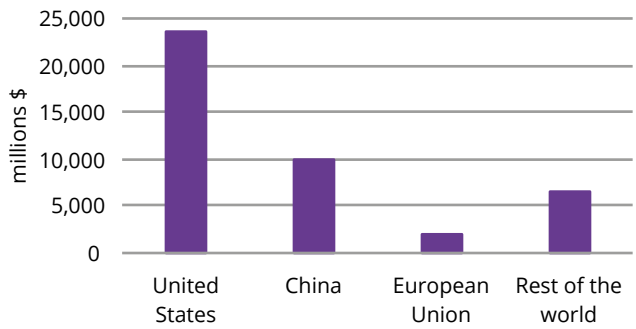
EU is trying to develop legislation that paves a third way between the other two models, promoting what is dubbed as "ethical and trustworthy AI". Its strategy is to foster cooperation between the public and private sectors, as well as ensuring a set of values that are considered to be key (e.g., transparency, accuracy, robustness and non-discrimination)[30]. However, in comparing the EU to China and the US, a pattern of a clear competitive disadvantage seems to emerge.

The huge gap in the overall amount of investments appears to be the most important reason for Europe lagging behind. According to Stanford University estimates[31], in 2020, the US continued to hold a dominant position in private AI investments. US companies invested $23.6 billion in AI, compared to China's $9.9 billion. Chinese investments in 2020 were less than half that of the US. It is important to note, however, that China has strong public investments in AI. In fact, both the central and local governments in China are spending heavily on AI R&D. The level of European private investments, on the other hand, is much lower and amounts to only $2 billion (Fig. 1.4.4).

Moreover, the US and China account for most AI start-up investments. Together, US-based and Chinese start-ups represented over 80% of the monetary value of VC investments in AI start-ups. In 2020, VC investments in US AI firms reached $45,000 million, instead, in Chinese AI start-ups they reached $19,000 million (Fig. 1.4.5).

Fig. 1.4.4 Private investment in AI by geographic area (2020)

Source: Artificial Intelligence Index Report 2021, Stanford University



The US and China were followed by the EU-27 that represented almost 5% of the value of VC investments in AI start-ups, while the UK start-ups made up for a little more than 4% of the total value[32].

Moreover, **also in terms of AI research publications and patents, the EU lags behind the US,** which led in AI publications with over 150,000 publications. China and the EU-27,did not exceed 140,000 publications (Fig. 1.4.6)[33].

In terms of patents, the EU-27 with about 3,000 AI patents registered in 2021 ranks second after the US (Fig. 1.4.7).

Moreover, if we analyse the situation at the level of single Member States, we find quite large differences, with some countries able to keep pace even at the international level, and others not very inclined to fully adopting AI.

30 PromethEUs, THE N(EU) WAY TO ARTIFICIAL INTELLIGENCE (2020)
31 https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf
32 https://www.oecd.org/digital/venture-capital-investments-in-artificial-intelligence-f97beae7-en.htm
33 https://oecd.ai/en/data-from-partners?selectedArea=ai-research

Fig. 1.4.5 Estimated VC investments in AI start-ups, by country (2012-2020)

Source: OECD.AI, Policy Observatory (2021)

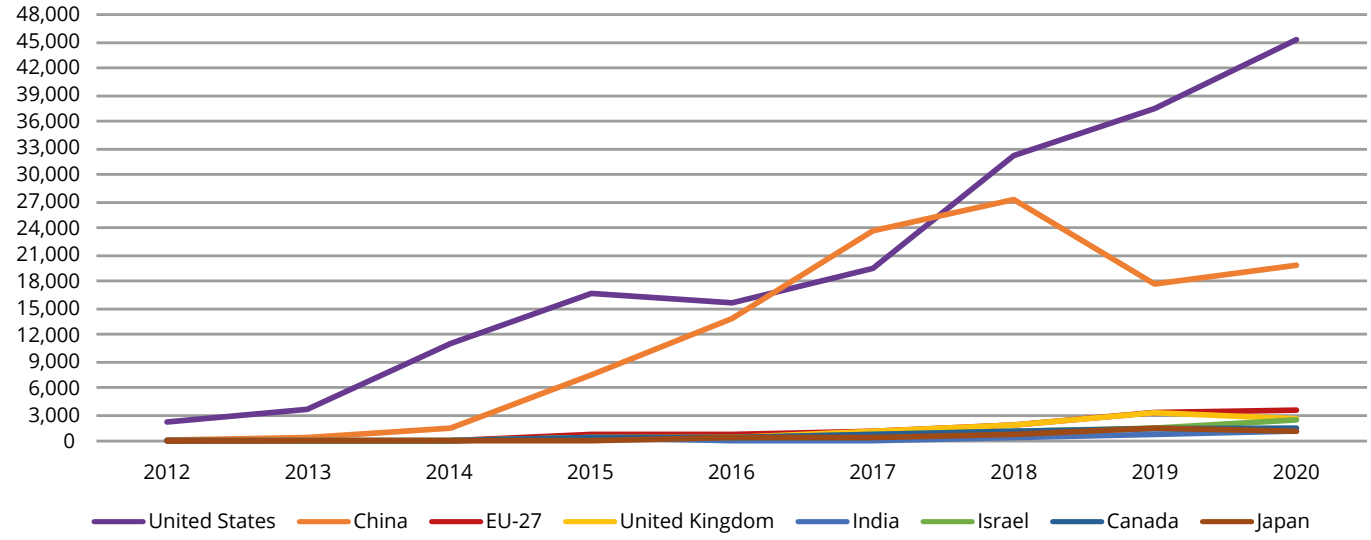


Fig. 1.4.6 Number of AI research publications, by country (2021)

Source: OECD.AI, Policy Observatory (2021)

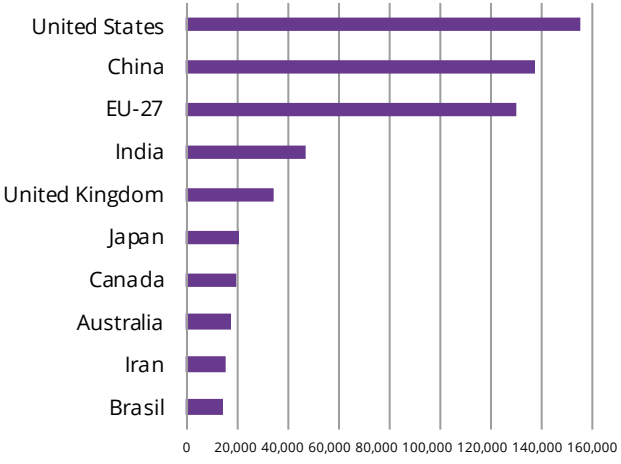
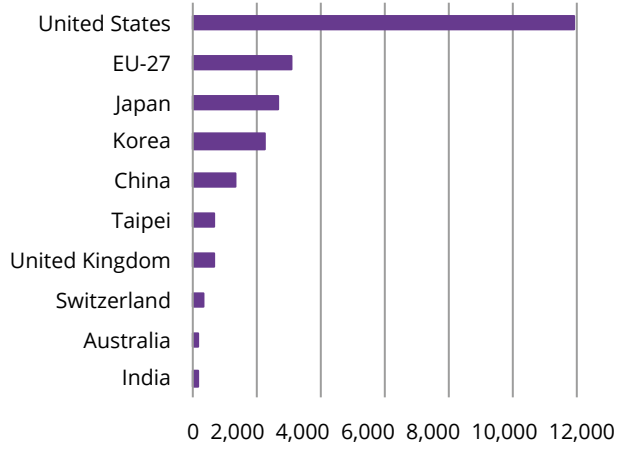


Fig. 1.4.7 Number of AI patents, by country (2021)

Source: OECD.AI, Policy Observatory (2021)



To provide an idea of the degree of AI development in European countries, I-Com has developed a new synthetic index (Fig. 1.4.8) that takes into account some variables relating to the industrial and research AI ecosystem in the various MSs, as well as the level of the adoption of some AI technologies:

- Number of AI firms (per capita value)
- Number of AI research institutes (per capita value)
- AI patent applications (per capita value)
- Enterprises that use 3D printing (in % of enterprises)
- Enterprises that use service robots (in % of enterprises)
- Enterprises that use industrial robots (in % of enterprises)
- Enterprises that analyse big data internally using machine learning (in % of enterprises)
- Enterprises that analyse big data internally using natural language processing, natural language generation or speech recognition (in % of enterprises)
- Enterprises with a chat service where a chatbot or a virtual agent replies to customers (in % of enterprises)

Each listed variable was appropriately weighted and an average of the variables was calculated for each country. The values obtained were normalised with respect to the country "best performer", in order to establish a ranking from 0 to 100.

On the top of the ranking, we find Ireland with a score of 100, followed by Malta and Finland with scores of 95 and 78, respectively. These countries, despite being small in terms of population – altogether they slightly exceed 11 million inhabitants – have a good AI ecosystem. Above all, Ireland is emerging as a leading player in AI[34] with 273 AI firms, many having filed patent applications. Moreover, Ireland has a much higher percentage than the European average (2%) of enterprises that analyse big data internally using machine learning (20%). Malta and Finland also have much higher percentages of enterprises than the European average using machine learning for the analysis of big data and using chatbot or a virtual agent to reply to clients. Germany (with a score of 44) and France (38) follow well behind. The two main EU countries in terms of AI firms, are far from the podium as, with respect to their size, the industrial and AI research ecosystem is not yet fully developed and the use of AI technologies by total enterprises is very low.

At the bottom of the ranking, we find the countries of Eastern Europe, where both the industrial and research AI ecosystem sees a lower number of active AI players or where the level of adoption of technologies is very low.

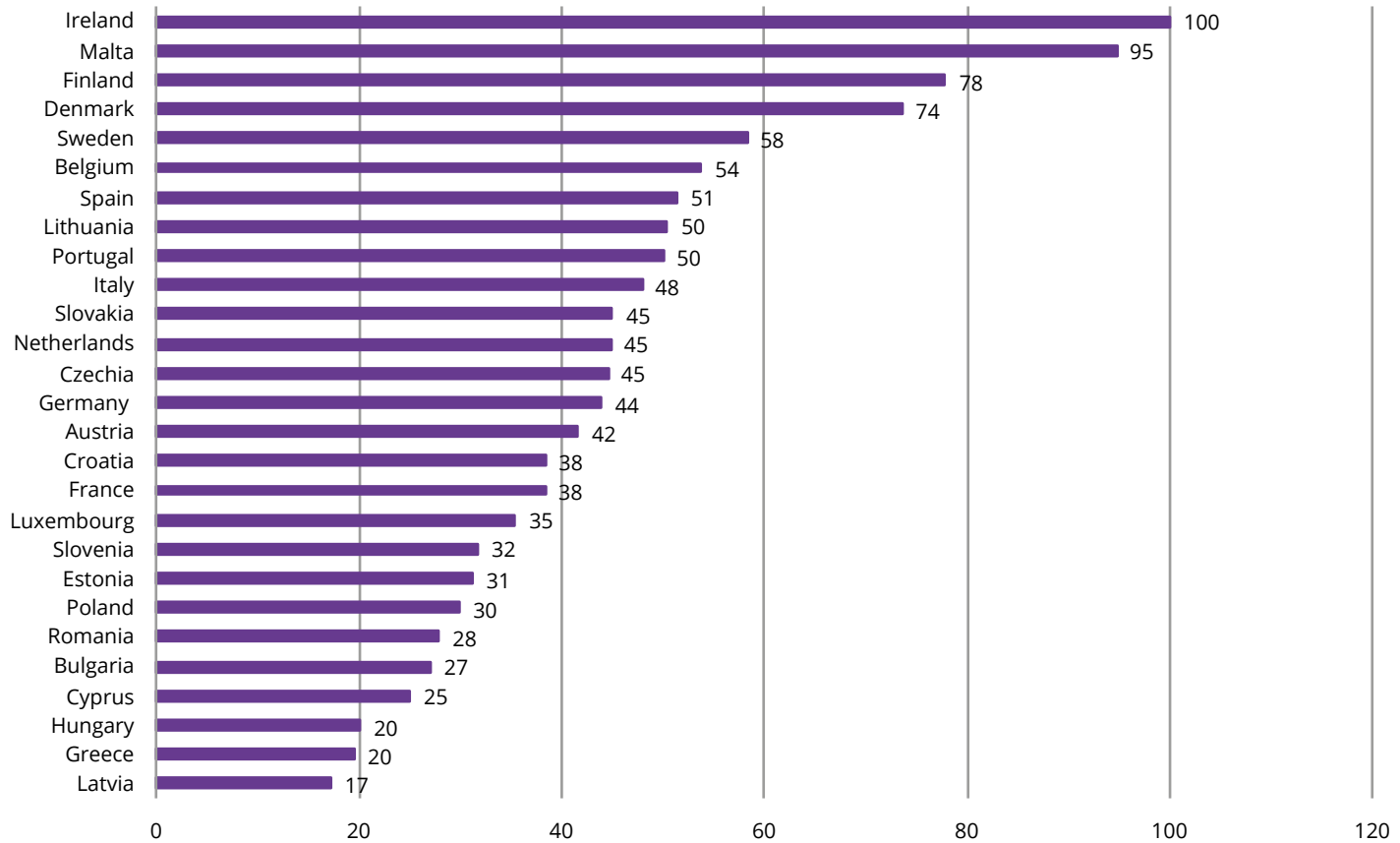
1.4.4. The EU legal framework on AI: the main milestones until 2020

The current historical period has been described as being on "the verge of the fourth industrial revolution", with the abundance of data combined with powerful algorithms and AI being the key element. Compared to previous industrial revolutions, today's digital revolution is on an unprecedented scale and with the enormous impact of emerging technological breakthroughs on states, economies, and societies.

34 https://www.trade.gov/market-intelligence/ireland-artificial-intelligence

Fig. 1.4.8 I-Com 2021 Index on AI development in European countries

Source: I-Com elaboration on Eurostat and EU Commission data



For this new revolution, it has been observed that Europe, which for a long time had dominated technological progress and set international standards, is slowly falling behind in this new 'winner-takes-most' economy, thus leading to European values being replaced and European companies marginalised. Despite the fact that the EU's interest and actions in the field of AI have been longer, the start of the EU's pro-active approach to AI regulation can be set on 25 April 2018, when the European Commission presented the Communication "AI for

Europe", the official kick-off of EU's actions in this field. One year before this communication was presented, the European Parliament adopted, in February 2017, a **resolution with *recommendations to the European Commission on Civil Law Rules on Robotics***, which described how an incremental use of AI would have been beneficial for many fields and especially the job market. Later that year, in May 2017, the EC published its mid-term review of the Digital Single Market Strategy where it underlined the importance of boosting Europe's scientific and industrial strength in order to reach a leading role in AI technologies, platforms and applications.

As previously mentioned, 2018 marks the start of the EU's new approach to AI. It was based on three main pillars: (a) placing the EU at the cutting-edge of technological developments, encouraging the uptake of AI by both the public and private sectors, increasing the EC annual investments in AI by 70% under the Horizon 2020 Research and Innovation Programme, strengthening AI research centres across Europe and supporting the development of AI applications in key sectors; (b) preparing the EU for socio-economic changes brought about by AI, supporting business-education partnerships to attract and keep more AI talent in Europe and implementing training and retraining schemes for professionals; (c) ensuring an appropriate ethical and legal framework.

Another important step along the EU's new path was the appointment of several experts to the High-Level Expert Group on Artificial Intelligence (AI HLEG) by the EC, in June 2018. In the same month, the EC also launched the AI Alliance, a multi-stakeholder forum to provide feedback to the AI HLEG. The AI HLEG's role was, and still is, to support European institutions in the implementation of the EU Communication on AI published in April 2018 and present plans on how to deal with mid- and long-term challenges and opportunities related to AI. In 2019, the AI HLEG presented the ***"Ethics Guidelines for Trustworthy AI"*** to provide guidance to all stakeholders and set a framework for achieving trustworthy AI.[35] According to the guidelines, trustworthy AI should be: (a) lawful, complying with all applicable laws and regulations; (b) ethical, ensuring adherence to ethical principles and values; and (c) robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm. According to said guidelines, each component is necessary, but not sufficient, for the achievement of trustworthy AI, thus, ideally, all three components should work in harmony and overlap in their operation.[36]

A few months later, in June 2019, another report entitled ***"Policy and investment recommendations for trustworthy Artificial Intelligence"*** was published by the AI HLEG group. The report highlighted the need for: (a) boosting the uptake of AI across sectors in the EU, and the need for higher investments in the field, (b) fostering

35 "Ethics Guidelines for Trustworthy AI", Directorate-General for Communications Networks, Content and Technology (European Commission), available at: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

36 The publication of the guidelines was preceded by a first draft of the document in December 2018, on which more than 500 comments were received through an open consultation. Results of said consultation are available here: https://ec.europa.eu/futurium/en/ethics-guidelines-trustworthy-ai/stakeholder-consultation-guidelines-first-draft.html

and scaling up AI solutions by enabling innovation and promoting technology transfer; (c) setting up public-private partnerships to foster sectoral AI ecosystems

Moving on, the start of the Von der Leyen Commission's commitment to the digital field can be identified in the publication of several proposals in February 2020. These proposals include, first of all, two communications – "Shaping Europe's digital future" and "A European Strategy for Data". The first communication sets three objectives ensuring the EU's digital transformation respects the core European values: (a) a technology that works for people; (b) a fair and competitive economy, (c) an open, democratic, and sustainable society. The second communication's aim is to make Europe a leader in the data economy, providing for a single market for data and a larger role for European companies. This communication also points out some of the major issues holding the EU back in the so-called "global AI race": (a) availability of data; (b) imbalances in market power; (c) data interoperability and quality; (d) data governance; (e) data infrastructures and technologies; (f) empowering individuals to exercise their rights; (g) skills and data literacy; and (h) cybersecurity.

Secondly, the Von der Leyen Commission's proposals included the **White Paper "Artificial Intelligence: a European Approach to Excellence and Trust"** to create an "ecosystem of excellence" and an "ecosystem of trust" for AI. For the first ecosystem, the EC wanted to revise the 2018 Coordination Plan and manage to guarantee that at least one digital innovation hub per MS had a high degree of specialisation in AI. For the other ecosystem, the EC tried assessing the main risks associated with AI. According to the white paper, AI applications must be deemed as high-risk when two cumulative criteria are met: (a) the AI technology is employed in a sector where, given the characteristics of the activities typically undertaken, significant risks can be expected to occur (for instance, healthcare, transport, energy and parts of the public sector); (b) the AI application in the sensitive sector is used in such a manner that significant risks are likely to arise. Moreover, the white paper cleared that the use of AI applications for employment processes, biometric identification and other intrusive surveillance purposes would always be considered as high-risk. Where an AI application falls under the category of "high-risk", some mandatory requirements were established in the following areas: 1) training data; 2) data and record-keeping; 3) information to be provided; 4) robustness and accuracy; 5) human oversight; 6) specific requirements for certain specific applications, such as biometric identification. The EC made it clear that such requirements would be partially verified through ex-ante conformity assessments and ex post controls that could be enforced by national authorities. Moreover, in the case of non-high risk AI applications, a voluntary labelling scheme, allowing the economic operators to signal the trustworthiness of their products or services would be applied.

1.4.5. The EU Commission's regulatory approach for AI: an overview on the "AI Act"

In April 2021, the European Commission presented the "AI Package" made up of three documents – a

Communication on Fostering a European Approach to Artificial Intelligence, the 2021 update to the Coordinated Plan with Member States, and a proposal for an AI Regulation laying down harmonised rules for the EU (AI Act). It has been observed that through the AI Package the European Commission intends to achieve another GDPR-like 'Brussels effect', using the EU's regulatory and market power to gain a competitive edge in the field of AI. The idea is that, through establishing the world's first AI all-encompassing regulatory framework, it could lead to a first-mover advantage and, thus, help establish leverage in exporting 'trustworthy AI' around the world and creating a set of international AI standards based on European values.

The aim of the Coordinated Plan is to use funding to: (a) create enabling conditions for AI development and uptake through the exchange of policy insights, data sharing and investments in critical computing capacities; (b) foster AI excellence 'from the lab to the market' by setting up a public-private partnership, building and mobilising research, development and innovation capacities, and making testing and experimentation facilities as well as digital innovation hubs available to SMEs and public administrations; (c) ensure that AI works for people and is a force for good in society by being at the forefront of the development and deployment of trustworthy AI, nurturing talents and skills by supporting traineeships, doctoral networks and post-doctoral fellowships in digital areas, integrating trust into AI policies and promoting the European vision of sustainable and trustworthy AI globally; and (d) build strategic leadership in high-impact sectors and technologies, including the environment, by focusing on AI's contribution to sustainable production, health by expanding the cross-border exchange of information, as well as the public sector, mobility, home affairs and agriculture, and robotics.[37]

However, it has been pointed out that the key part of this package is the proposal of an **Artificial Intelligence Act**.[38] The latter has been described as "the first ever legal framework on AI" and its aim is to set out horizontal rules for the development and use of AI-driven services, systems and technologies within the EU borders. With the AI Act proposal, the EC tried to translate the "trustworthy AI paradigm" into a set of rules for the EU. According to this paradigm, AI technologies must be ethically, technically and legally valid, while, at the same time, respecting those democratic values, human rights and the rule of law that constitute the basis of the EU. Therefore, the goal is to create an environment of trust among European citizens with regards to AI. The regulation outlines a four-level approach to regulating risks posed by AI systems, with different sets of rules and obligation applying to each level.

First of all, the proposal identifies a list of prohibited uses of AI technology due to their **"unacceptable risk"** (art. 5). The ban regards AI applications such as certain types of social scoring and biometric surveillance which constitute

37 See: https://digital-strategy.ec.europa.eu/en/policies/plan-ai

38 Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on AI (Artificial Intelligence Act) and amending certain Union legislative acts – COM(2021) 206, see: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

a threat to privacy, non-discrimination principles and related human rights. The proposal also partially bans law enforcement uses of "'real-time' remote biometric identification systems" in public spaces (with the broad exception of "strictly necessary" cases).

Secondly, there are the so-called **"high-risk"** AI systems (art. 6 and 7 of the proposal) that include those used to identify and categorise people based on their biometric data, and manage access to social security benefits and other social services, which would require extra safeguards to deploy. The AI Act defines specific rules and obligations for this type of AI technology, such as implementing: (a) a risk management system to eliminate or reduce risks of design and development; (b) mitigation and control measures; (c) providing information and training, and conducting testing It should be noted that the the obligations imposed on those involved in the production of high-risk AI differ among the players involved and, therefore, among providers of high-risk AI systems, product manufacturers, authorised EU representatives appointed by non-EU providers, importers, distributors, users, and other third parties involved in the AI value chain.

The providers of high-risk AI systems are responsible for verifying that their AI systems comply with the AI Regulation, implement a quality management system, draw up the relevant technical documentation, keep logs generated by their high-risk AI systems, comply with conformity assessment and registration obligations, take corrective actions as required and cooperate with authorities. Manufacturers of products covered by EU legislation are responsible for compliance as if they were the provider of the high-risk AI system. Distributors, importers, users and other third parties will also be subject to providers' obligations if they place a high-risk AI system on the market or into service under their name or trademark, modify the intended purpose of a high-risk AI system already on the market or in service or make a substantial modification to a high-risk AI system. The proposal also identifies some obligations for users of high-risk AI systems. Those using this type of technology will have to do it in accordance with the instructions for use, ensure that input data is relevant, and monitor the operation of the high-risk AI system based on the instructions. For ex post surveillance, providers of high-risk AI systems will have to establish a post-market monitoring system in order to verify their compliance with the regulatory requirements. In addition, such subjects will have to report to the market surveillance authority of the MS any serious incident or malfunctioning.

Thirdly, the proposal identifies **"limited-risk"** AI systems (art. 52) which include AI applications such as biometric categorisation, emotion recognition and deep fake systems. Such systems do not require the same procedures as high-risk ones, and the providers of such technologies have less obligations compared to developers of "high-risk AI". Finally, "minimal-risk" AI applications can be defined as a residual category that includes all the AI systems which are not covered by specific requirements and safeguards in the discussed proposal.

Furthermore, the AI Act proposal establishes a **European Artificial Intelligence Board**, which will be made up of

representatives from the MSs and the EC. The aim of the Board will be to facilitate a harmonised implementation of this regulation and enhance the cooperation between national supervisory authorities, provide advice and guidance to the Commission, and "collect and share" best practices from MSs.[39]

1.4.6. The European and international debate around the EC proposal for a regulation on AI

Since the EC presented its new proposals in April 2021, the proposal for an AI Act has been surrounded by an **increasing debate both at a European and international level**.

While, on the one hand, stakeholders and experts have praised the Commission for its efforts to lay down a harmonised framework for AI, on the other, it has been pointed out that the EU will not be able to truly establish itself as a global leader in the field of AI regulation, unless it first achieves a leading role in the development of AI technologies. Moreover, stakeholders and experts feel that, if the race in AI development accelerates and the gap between the EU and the other countries becomes even wider, this will most certainly affect the chances for the EU to establish itself as a leading force in the regulatory framework for AI.

With the AI Act, European institutions are called on to answer several complex questions – How to protect people from potential harmful uses of AI. How to define AI and risky AI without being too broad or too narrow. The need to protect consumers and clearly define their rights when it comes to harm caused by AI technologies., and so on. Moreover, as revealed by the public consultation carried out by the European Commission, there is a widespread appreciation among stakeholders when it comes to the focus on human rights, and the explicit goal to create a regulatory framework that will be able to protect them in the field of AI.

Experts have underlined that the EU regulatory approach strongly focuses on ethical considerations and aims at establishing a regulatory framework in line with core human rights and democratic principles. More specifically, it has been stressed how crucial it is that EU institutions continue to thoroughly analyse the proposal while,, at the same time try to pursue a better coordination in AI regulation. A key element in this cooperation would be a closer collaboration between the private and the public sectors.

In addition, it has been pointed out that an enhanced dialogue and exchange between the EU institutions and national authorities should be promoted before provisions at different levels end up pursuing different goals or even contradicting each other. Hence, the possibility of a multilateral governance approach has emerged from the public debate, and it seems to many as a viable option that should be further studied.

Where more recent developments are concerned, at the beginning of October 2021, the use of AI technology by the police and judicial authorities in criminal matters was discussed during a plenary session in the European

39 At national level, MSs will have to designate one or more national competent authorities and establish a national supervisory authority with the task to supervise the implementation of the regulation.

Parliament. During this discussion a report on AI in criminal matters was presented. Although not binding, this report is an important addition to the debate surrounding the AI Act and the risk-based approach chosen by the EC. It outlines several principles that should be pursued in the use of AI technologies in this field, such as fairness, data minimisation, accountability, transparency, non-discrimination and clarity. According to a study presented in the EU Parliament at the end of the same month, police in several EU countries (Austria, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Slovenia, and the Netherlands) already employ facial recognition technologies for ex-post identification.[40] Finally, an interesting addition to the debate came on the 9 November 2021, when the draft report of the Special Committee on Artificial Intelligence in a Digital Age was presented and first discussed.[41] The aim of this report is to explore the impact of AI on the European economy throughout different sectors. The report stressed how AI companies based or operating in the EU often face legal uncertainty regarding the development their products and services and that the digital single market lacks established clear AI norms. At the same time, according to the paper, excessive safety standards and bureaucratic burdens could lead to inefficiency and lower investments as, at this moment, the success of a new AI technology is not yet foreseeable compared to the risk of the high initial investments.

To conclude, the debate around the Commission's AI Act proposal is certainly active, with different perspectives and voices. The proposal has been praised by stakeholders and experts for its ambitious goal to regulate such a fast-moving field, yet at the same time, many have expressed their concerns on how this regulation should deal with specific and controversial aspects of AI technology and its application within the EU borders.

40 Report for the Greens, "Biometric & Behavioural Mass Surveillance in EU Member States", EFA in the European Parliament October 2021.

41 Special Committee on Artificial Intelligence in a Digital Age – Draft Report On Artificial Intelligence In A Digital Age (2020/2266(INI)). The final report will be the primary output of the committee work, and the full version is due next spring. See: https://www.europarl.europa.eu/doceo/document/AIDA-PR-680928_EN.pdf

1.5. 5G NETWORKS IN THE EUROPEAN UNION

1.5.1. The development of 5G networks in Europe and the rest of the world

Throughout 2021, Europe has taken a number of important steps towards the development of 5G networks. Among these, significant improvements have been made in the allocation of a large number of frequencies through national auctions, and in the launch of innovative services by a large number of operators. These have strongly helped to shape the market and to reach to large parts of the EU population, and **5G services are now available in all EU-27 countries with the exception of Portugal and Lithuania**.

Alongside the UK,, the first country with four operators out of four to provide 5G services, Denmark, France, Italy, Spain, and Sweden now also **provide full coverage** (all with four active operators out of four) in terms of 5G network availability. Austria, Finland, Greece, Ireland, Luxembourg, the Netherlands and the Czech Republic are also quickly developing their domestic infrastructures, with three fully equipped operators in each of these countries providing 5G services.

Overall, the EU appears keen to match the progress in 5G services that is taking place around the world. According to EU 5G Observatory estimates, more than 180 operators had already launched 5G services by June 2021 (marking an increase of +100 operators compared to June 2020), highlighting the major developments taking place in the sector. In the US alone, the four largest operators had already launched fifth generation services between 2018 and 2019, while in South Korea and China, the three largest local players are also already providing 5G connectivity. Similarly, in Japan, three 'incumbent' operators (NTT Docomo, KDDI and Softbank) started offering the service in March 2020, while newcomer Rakuten launched it last September.

Europe's attention on developing 5G networks and, in general, on wanting to renew existing services in order to face the global economic and technological challenges, started in 2016 when the Commission launched the **5G Action Plan (5GAP)**. Its aim was to boost EU efforts for the deployment of 5G infrastructures and services across the Digital Single Market by 2020, with the ultimate goal of ensuring the achievement of a comprehensive continental coverage by 2025. At the end of March 2021, the Commission published a **Connectivity Toolbox,** including 39 best practices from MSs. According to the plan, by the 30 April 2021, every EU MS should have provided the Commission with a roadmap for the implementation of the toolbox while, by the 30 April 2022, all MSs will have to report on the implementation of the toolbox. The aim of the strategy is to foster the deployment of 5G infrastructure by promoting major uniformity and by reducing both costs and burdens arising from regulatory issues.

In terms of 5G trials on the so-called **"*Pioneering*" spectrum bands**[42] (700 MHz, 3.4-3.8 GHz, 26 GHz), in June 2021, the

42 The 5G pioneer bands identified at EU level are the 700 MHz (694-790 MHz), the 3.6 GHz (3.4-3.8 GHz) and the 26 GHz (24.25-27.5 GHz) frequency bands. The technical conditions of the three 5G pioneer bands have been harmonised through Commission Implementing Decisions (EU) 2016(687) of 28 April 2016, 2019/235 of 24 January 2019 and 2019/784 of 14 May 2019 respectively. The last one, which concerns the 26 GHz band, has been amended by Commission Implementing Decision (EU) 2020/590 of 24 April 2020 to take due account of the developments at the last ITU World Radio-communications Conference in 2019. (EU 5G Observatory, 2021).

most widely tested frequency band in Europe was by far the **3.6 GHz** (69% of tests). The percentage of assigned spectrum for this is almost 55% at continental level, whereas only 46% of the spectrum in the **700 MHz** band has been assigned. Values are instead much smaller for the **26 GHz** band, which is being deployed at a much slower pace and for which 80% of the spectrum still has to be assigned.

Finland, Germany and **Greece** are the most advanced countries in terms of assigned spectra, with all **pioneer frequencies allocated** by June 2021. These are closely followed by Denmark and Slovenia, while several other countries have allocated about two-thirds of their frequency resources in the indicated bands. Among these, Cyprus, the Czech Republic, Austria, Slovakia, Luxembourg and Hungary, as well as Italy, where the allocation of the 700 MHz bands had been completed several years ago but its entitlement is only scheduled to start in July 2022. Instead, **the EU-27 average percentage of assigned spectrum is lower (**only **45.8%)**, as a number of countries still present impacting delays. Among the other larger countries, France is in line with the continental average, and has allocated about a half of its bands, while Spain is lagging behind, and has only allocated a third. Several smaller countries, such as Croatia, Poland, Estonia, Lithuania and Malta, are still waiting to start the allocation procedures.

Instead, in terms of completion of the auctioning procedures, Bulgaria, Denmark, Spain, Slovenia and Sweden have all completed their **national auctions** in the current year.

The effects of a widespread availability of 5G networks also have to be measured and evaluated in terms of **access** to these by households. Although, on the one hand, this data suggests a good degree of "5G readiness" (Fig. 1.5.1), with frequency assignment procedures having been completed in many cases, on the other, there is a certain lagging behind in 5G coverage. Data from Eurostat's **Digital Scoreboard**, which tracks the evolution of relevant indicators on Europe's digital performance across EU MSs (and others, i.e., Norway), show that **fewer than 14% of European households had access to 5G mobile broadband coverage in 2020**. The only countries where 5G coverage was at least 80% were Denmark and the Netherlands, followed by Austria and Ireland with 50% and 30%[43]. Instead, as many as 15 countries did not have 5G coverage by 2020 (Fig. 1.5.2).

These existing shortcomings that are present in most countries in terms of 5G supply can, however, rely on very **high levels of 4G mobile broadband coverage**, which has been growing strongly in availability to households over the last eight years. Starting from 2018-2019, the supply of 4G reached an average coverage of more than **90% of households** in all European countries, including rural areas. On the basis of a methodological normalisation provided by the EU 5G Observatory[44], a comparison can also be made with the allocation status of the other main countries at world level[45]. Taking into account that non-

43 These values published by Eurostat do not provide any specification on the type of 5G infrastructures, namely, if the architecture of the network is Non-Standalone (NSA) or Standalone (SA). Further specification on this distinction is provided infra.

44 Benchmark used by 5G Observatory for comparison. Source: 5G Observatory, Quarterly report no. 12, June 2021.

45 USA, China, Japan and South Korea with the EU-27 and the UK.

Fig. 1.5.1 5G readiness (EU-27)

Source: 5G Observatory, June 2021

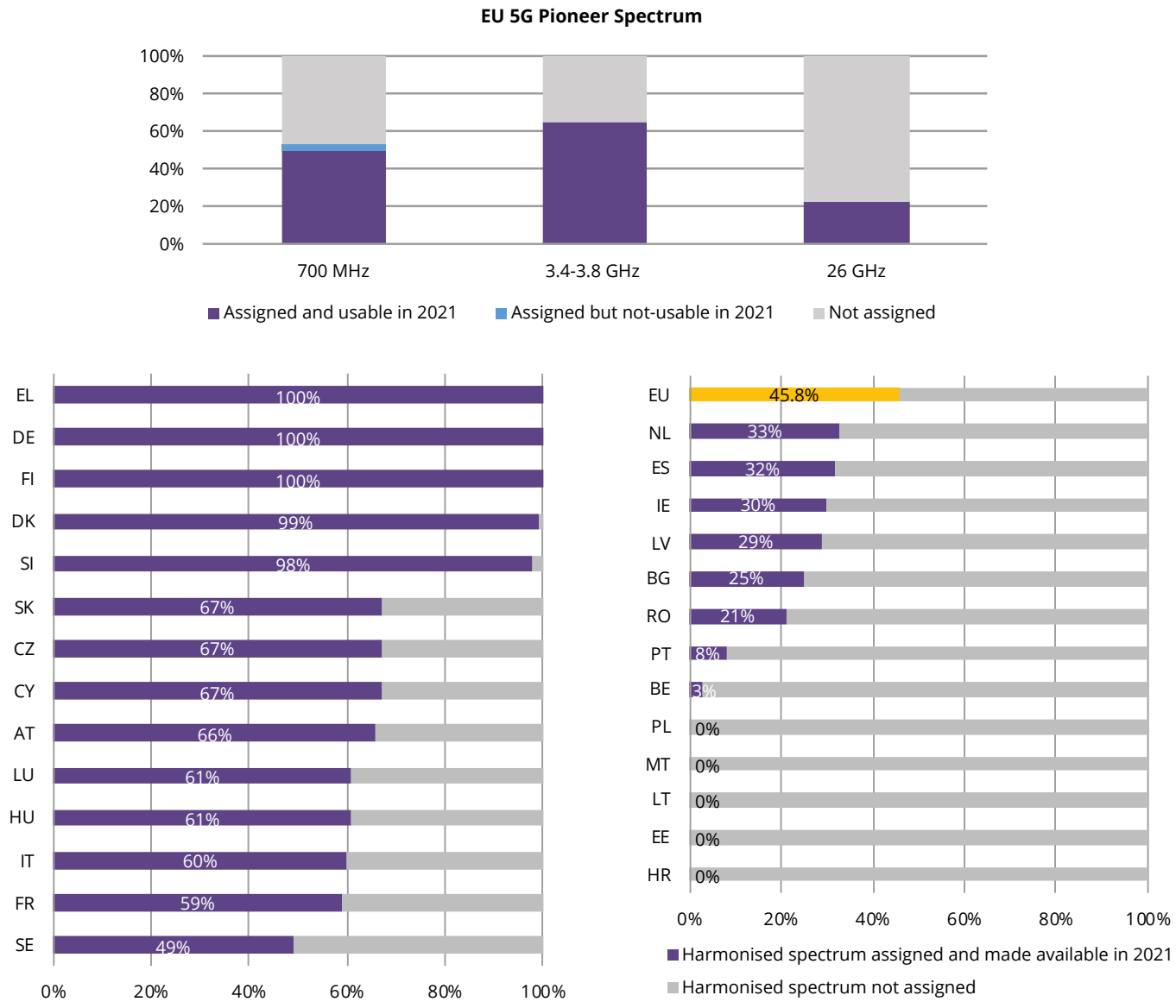
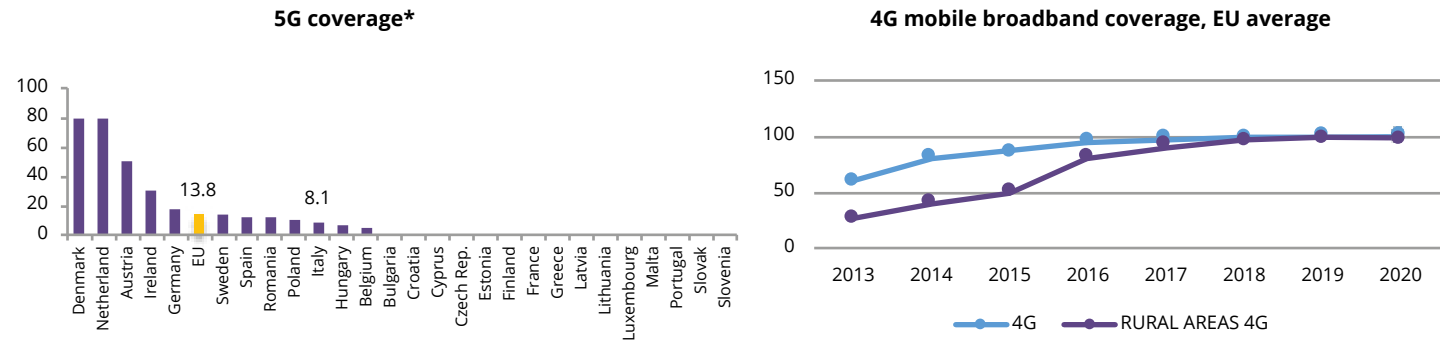


Fig. 1.5.2 Coverage in Europe (as a % of households, 2020)

Source: Eurostat, 2020



* Eurostat definition: *"Coverage is a supply indicator defined as the percentage of Households living in areas covered by fifth generation mobile broadband. Source: IHS Markit, Omdia, Point Topic and VVA, Broadband coverage in Europe studies"*. No distinction is made between NSA and SA infrastructures.

European countries do not follow the EU's specification in identifying explicit "pioneering 5G bands", the graphs presenting a **worldwide comparison** show the amount of identified and assigned spectra in terms of *low frequency bands*, *mid frequency bands* and *high frequency bands*[46].

For comparison purposes, the classification used by the EU 5G Observatory and illustrated in Fig. 1.5.3 distinguishes frequency levels that are lower than 1GHz (low frequency bands), between 1 GHz and 6 GHz (medium frequency bands) and above 6 GHz (high frequency band). Furthermore, country-specific distinctions are also made and taken into consideration in some cases. In the US, for example, the 600 MHz band is considered as the low-frequency band, the mid-frequency bands are those between 2.5 GHz and 3.5 GHz[47] and the high-frequency bands are those between 24 GHz and 48 GHz[48]. South Korea also presents some specifications as the low-frequency

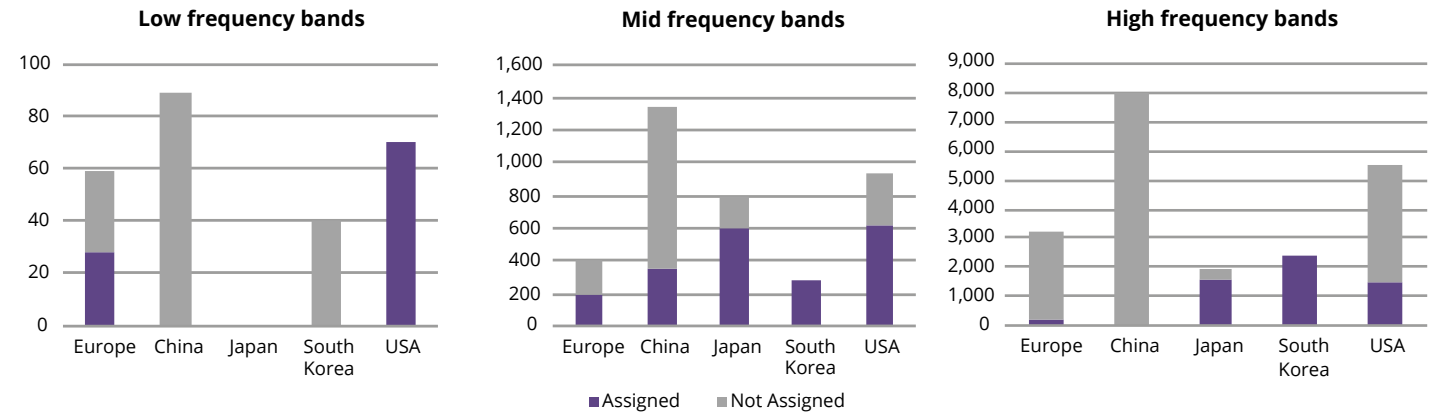
46 On a technical level, a *low frequency band* (i.e. an electromagnetic emission with a frequency <1GHz) allows the signal to reach longer distances compared to a *high* frequency one, but has the drawback of carrying less data per unit of time (calculated in Mbps or Gbps). On the contrary, a *high frequency band* frequency (in this case >6GHz is chosen as benchmark parameter) transfers a larger volume of data per unit of time, but presents a reduced range and level of intensity. In fact, while *low frequency bands* are able to cross physical obstacles, *high* frequencies are still strongly prone to disturbances and distortions caused not only by physical obstacles (houses, trees) but also by atmospheric agents (rain, clouds). Such features require two crucial elements to be considered in order to maximise the benefits of 5G: the implementation of a good number of aerials capable of guaranteeing high coverage, and the orientation of the devices with respect to the needs of the required service.
For example, the low band is better suited to low data-intensive connections such as those for smart homes, while the high band is more effective for data-consuming applications such as the online streaming of audio-visual content.

47 Specifically, 2500 MHz, 3550-3700 (CBRS), 3700-4200 and 3450-3550 MHz.

48 In The US the high-frequency bands are: 24250-24450, 24750-25250, 25250-27250, 26500-29500, 31800-33000, 37600-38600, 38600-40000, 42000-42500, 47200-48200 MHz.

Fig. 1.5.3 Assigned frequency bands (2021)

Source: 5G Observatory, June 2021



bands are the 700 MHz, medium-frequency 3420-3700 MHz and high-frequency 26500-28900 MHz bands. China also considers the low frequency band at 700 MHz, while the medium frequency bands are 2600-5000[49] MHz and the high frequency bands are 24750-27500 and 37000-42500 MHz. In Japan, no band below one Gigahertz has been identified, while at mid-frequency 3600-4200 MHz and 4400-4900 MHz have been identified, and among the high-frequency bands, 27500-29500 MHz.

In this comparative analysis (Fig. 1.5.3), Europe ranks second, behind the US, in terms of assigned **low frequency bands**. The latter has in fact allocated all of its identified spectrum compared to half of the identified 6 GHz allocated by the EU.

For **medium bands**, China and the US are planning to allocate the highest number of MHz to 5G in the coming years (more than 1,300 MHz in China and more than 900 MHz in the US), although, to date, Japan has had the largest portion of allocated frequencies in this band (600 MHz out of the identified 800 MHz). Europe, instead, has only identified 400 MHz (in the 3.4-3.8 GHz range), a half having already been allocated.

A different scenario concerns **high frequency bands**, where Korea and Japan have already allocated almost all of their identified spectra (2000 MHz and 2300 MHz respectively) while the other analysed countries, despite having identified many more, have allocated just a few. China, in particular, still has to start the allocation procedure of all its 8000 MHz in the high frequency band, and Europe has only done a little better. In fact, in June 2021, the 26 GHz band had

49 Specifically, 2600, 3300-3400, 3400-3600, 3600-4200, 4400-4500, 4800-5000 MHz

only been allocated in Italy[50], Germany[51], Denmark[52], Greece[53] and Slovenia[54].

The reported figures, however, do not take account of the structural differentiation in 5G networks in terms of **Non-standalone (NSA)** and **Standalone (SA) 5G** infrastructures. The former was strongly preferred in the transition period towards the full deployment of the 5G services, as operators could make use of techniques that allowed them to offer *'partial'* 5G services by simply upgrading previously installed fourth generation Radio Access Network (RAN) infrastructures. This allowed them to keep the core network (4G) unchanged, while offering a significant increase in performance. However, this hybrid architecture – which has dominated the sector over the last years – is now recognised as limiting, as it **does not allow for the maximum potential 5G performance to be fully exploited**.

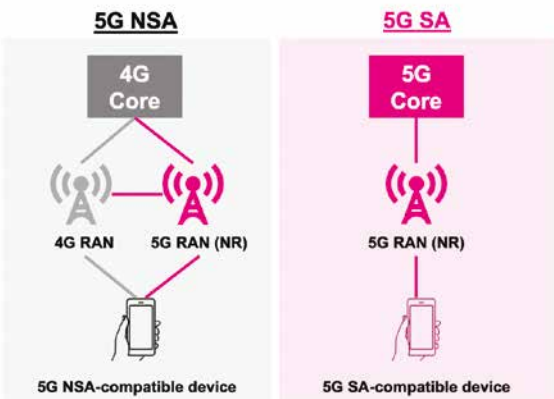
Standalone systems, instead, require a "pure" transition and evolution of the networks, which necessarily implies the adoption of next-generation infrastructures and equipment for both the access network and the core network (Fig 1.5.4). For the consumer market, 5G SA compatible devices would be provided with **better coverage and improved latency**, and devices connected to a low frequency band in 5G, but without connection to a 4G LTE (and thus EPC), could finally be covered directly in 5G. In NSA devices, in fact, the control plane is still mostly handled by the 4G Core network.

Although the European 5G Observatory (2021) states that **all advanced 5G markets in the world mainly still rely on NSA structures**[55], the deployment of SA infrastructures has started over the last year in a series of countries, such as China[56] and the US[57].

In the near future, most non-standalone 5G deployments are expected to be migrated to, or be augmented by additional, 5G standalone networks. Interest in SA architecture is increasing yearly, and this share could

Fig. 1.5.4 Standalone (SA) vs Non Standalone (NSA) 5G

Source: Rakuten



50 Assigned in October 2018.
51 From 2020 it is available on request at local level.
52 Assigned in April 2021.
53 Assigned in December 2020.
54 Two blocks were allocated in January 2018 but were not available for 5G and there was a further allocation in April 2021.
55 USA, China, Japan, South Korea.
56 In China, the three main MNOs have launched their SA network quite extensively. China Mobile for instance has deployed or upgraded 400,000 base stations to support SA mode and it plans to have 200 million 5G SA devices on its network in 2021.
57 In the USA, where T-Mobile has launched SA on the 600 MHz frequency band, a 30% increase in coverage was observed and latency was reduced by 24% as compared to 5G NSA.

expand considerably as network operators decide to start the deployment of a native 5G Core. As well as providing faster connection times (lower latency) and support for a massive number of devices, 5G SA is also of paramount importance as it enables a multitude of new functionalities beyond greater bandwidth for the support of new features such as network slicing and Machine Type Communication or Ultra-Reliable Low Latency Communications (URLCC).

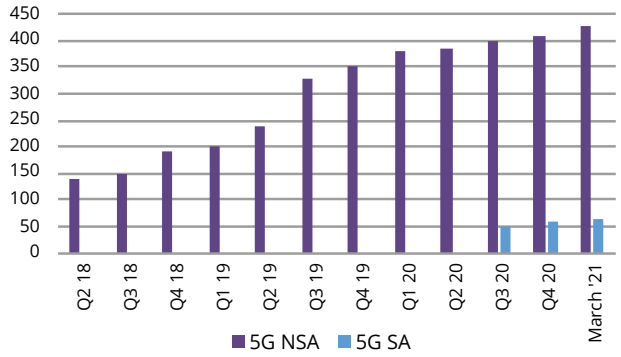
These developments have been reported by the Global Mobile Suppliers Association (GSMA), according to which at least seven operators[58] in five different countries have announced to have launched public 5G SA, and **68 operators in 38 countries worldwide have been more generally investing in public 5G SA networks**. Furthermore, as of February 2021, GSACOM reported a total number of **304 already announced 5G devices with support for 5G standalone**, 204 being commercially available.

As for the European context, no specific official data on SA is available. However, according to a survey commissioned from IDG by F5 which was conducted on a sample of 163 managers, **41% of mobile operators in Europe have deployed, or plan to deploy, a core network with 5G standalone architecture soon**, while **90% say they intend to complete the transition to 5G standalone by the end of 2023**. This last figure is in line with that reported in surveys concerning other regions – North America (96%), the Middle East and North Africa (94%) and Asia (86%) (GSACOM).

Fig. 1.5.5 The evolution 5G Standalone mode (March 2021)

Source: I-Com reconstruction of GSA (2021) data.

1.5.5 A - Number of operators investing in 5G SA at world level



1.5.5 B - Map of operators investing in 5G SA

* GSA (2021) – GeoNames. HERE, MSFT, Microsoft, Navinfo, Navteq, Thinkware Extract, Wikipedia

58 Including T-Mobile, Plus China Mobile HK, Rain (South Africa) and DirecTV (Colombia).

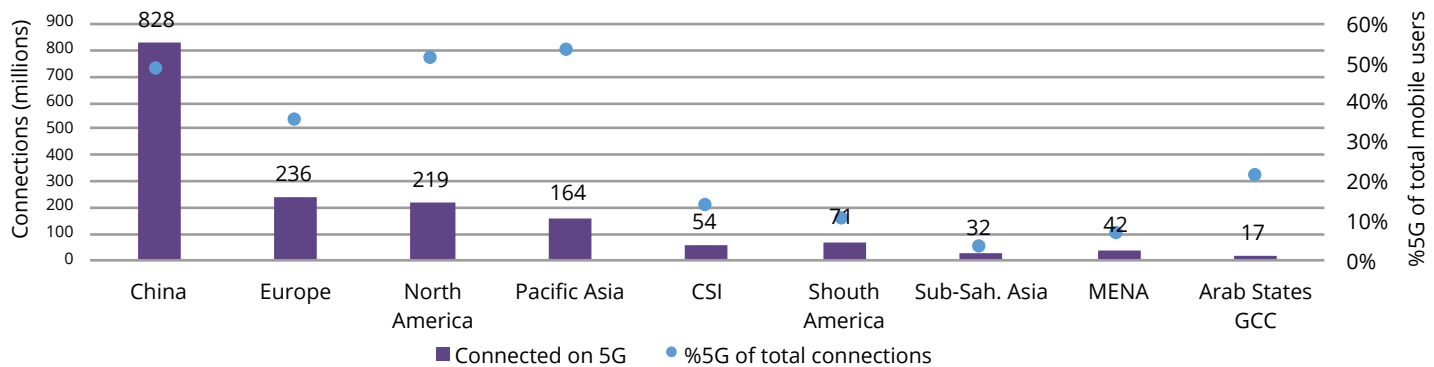
1.5.2. Consumer and enterprise adoption of 5G services

As structural investments are planned to increase over the following years, the demand for 5G services and networks is also expected to grow considerably. As stated previously, **the adoption of 5G is already accelerating worldwide** and, although nearly three in five connections at global level still make use of 4G technologies, about **8% of all connections are already being made on 5G**. The fifth generation network is now available, at least to some extent, in **every region of the world**[59], and is expected to be used for **more than 20% of all mobile communications at global level** by 2025[60]. According to GSMA's estimation (Fig. 1.5.6), the Asian countries will undergo a steady growth in 5G usage rates, eventually reaching more than a billion connections on 5G networks (of which more than 800 million in China and more than 160 million in the Pacific-Asian countries), compared to about 240 million connections in Europe and 220 million in the US. In proportional terms, the percentage of 5G usage is expected to be significantly lower in Europe (about **35% of total mobile users**) than in the US and Asia (up to over 50% of users).

A similar trend, possibly even further strengthened by the fact that the estimate extends to 2026, is reported in Ericsson's Mobility Report released in June 2021, in which the affirmation of 5G is shown in terms of number of **mobile phone subscriptions** (Fig 1.5.4). In fact, although Enhanced Mobile Broadband (eMBB) and Fixed Wireless

Fig. 1.5.6 5G connections by continental area (mln, 2025)

Source: GSA (2021)



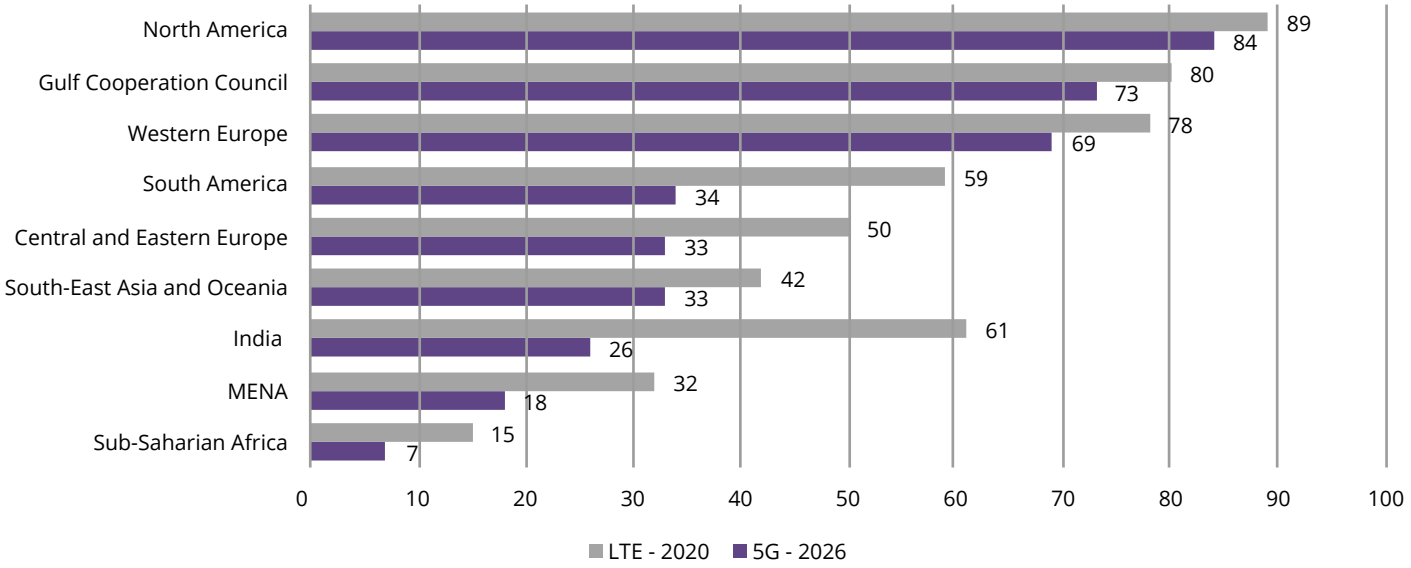
* The value for China includes Hong Kong, Macao, and Taiwan.

59 GSMA intelligence, June 2021.

60 According to the forecasts made by GDMA (2021), China alone will account for nearly half of the 21% total of 5G connections by 2025, while adoption will be highest in developed Asia-Pacific and North America.

Fig. 1.5.7 Mobile phone subscriptions, by continental area (2020 – 2026)

Source: Mobility Report, Ericsson (June, 2021)



Access (FWA) connectivity still remain the dominant 5G use cases, a vast variety of **5G-enabled smartphones** are now available on the market. These include products from some of the world's largest mobile producers, such as Apple[61] (USA), Xiaomi (China) and OnePlus (China).

This growing interest from producers is probably being fostered by changes in consumer preferences, as they seem increasingly interested in accessing the most efficient and effective networks on the market. According to a survey run by GSMA, the **majority of worldwide users intend to upgrade their mobile service to 5G networks** (Fig 1.5.8). 30% of all mobile users also responded that they would be willing to change provider, thereby probably incurring additional costs, if this were necessary in order to access the fifth generation networks. However, it is interesting to notice that almost a third prefer to wait for further developments on the market, highlighting that these network innovations still have room for further progress in terms of service availability, reliability, and spreading among customers.

Ericsson's Mobility Report also estimates that 160 service providers launched 5G commercial offerings

61 Apple launched the 5G-compatible iPhone 12 line of smartphones in late 2020.

in 2020 and that 5G device subscriptions grew by 70 million in the first four months of the same year (total 290 million), with an **estimated 580 million 5G mobile phone subscriptions to be reached by 2026**. As well as smartphones, 5G is also expanding to several other devices, for example, with new applications and form factors around **augmented and virtual reality** (AR/VR) technologies.

A marked increase in 5G adoption is also expected in the business sector, as new technologies such as IoT, IA and augmented reality, are becoming both essential in production and demanding in cutting-edge network services. According to a research conducted by Interdigital in 2020[62], only 11% of responding firms reported that a transition to 5G networks was not part of their business plans, while **60% state that they will adopt 5G within the next two years** – adding to the **12% that already make use of it**.

The sectors expected to benefit most from the application of 5G technologies are the automotive industry (both as the first choice, with 24%, and out of the top three, with 58%), followed by the manufacturing (46%), media (39%) and energy and transport (37%) industries.

62 Interdigital, Great Expectations: Sizing the Opportunity for 5G in Vertical Industries, 2020. The sample is made up of 41% from European firms, 28.6% from North America, 21.3% from Asia, 4% from the Middle East, 3.4% from Africa and 1.4% from South America. In terms of industry affiliation, almost 20% work for a mobile operator, just over 20% for network equipment vendors, 14% for system integrators and consulting firms, and almost 15% for vertical industries (education, financial services, energy and utilities, media, transport and logistics). The remaining come from software vendors (13%), device manufacturers (8%), other types of network product and service providers (5.5%) and virtual operators (MVNOs, 3.7%).

Fig. 1.5.8 Mobile users shifting to 5G networks (% of mobile users)

Source: GSMA (2021)

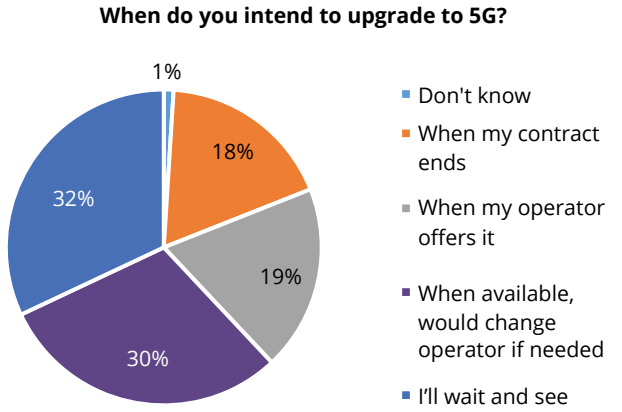
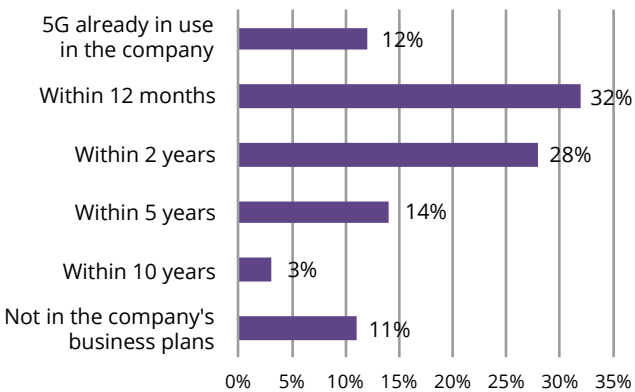


Fig. 1.5.9 Intention of adopting or applying 5G industrial technologies (%)

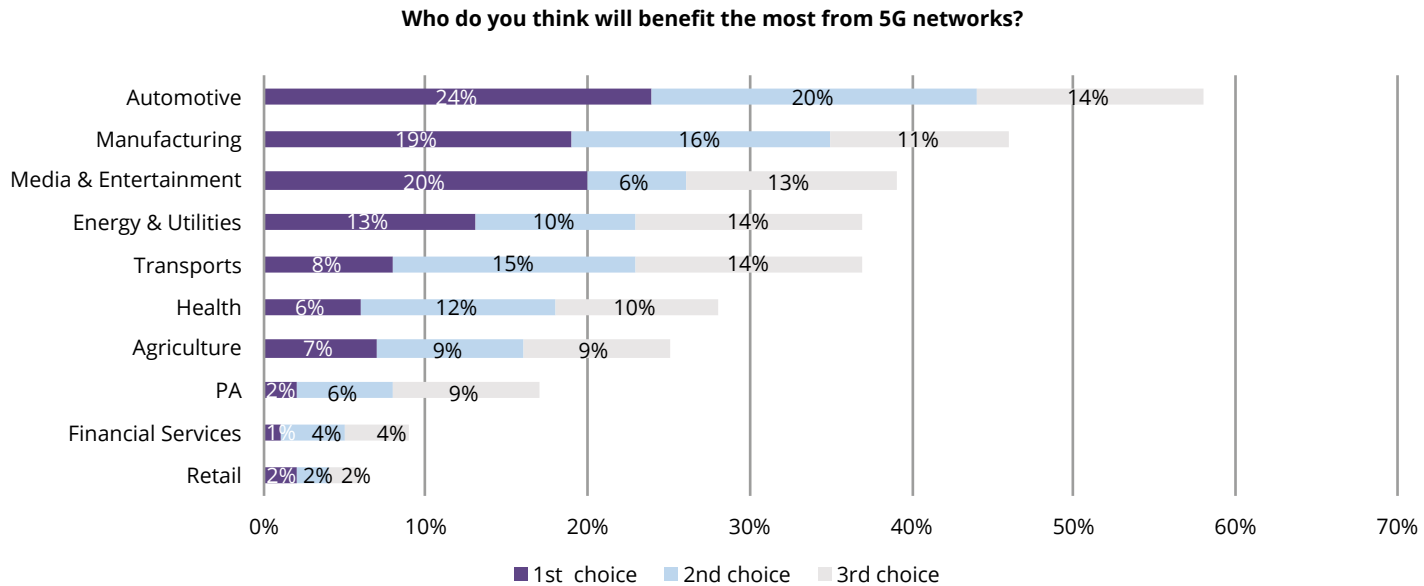
Source: Interdigital, 2020



Notes: The sample consists of 345 professionals from the mobile and vertical market communications industries.

Fig. 1.5.10 Industries that will benefit most from 5G in the next 2 years (% of respondents)

Source: Interdigital, 2020



Notes: The sample consists of 345 professionals from the mobile and vertical market communications industries

In many cases, firms have also set up their own 5G network over the last few years. In contrast with the so-called "Public networks", that are used to provide publicly available electronic communications services, **"Private networks"** (or campus networks) are defined as networks owned by private entities and only accessible to their employees, stakeholders and/or customers. Among European countries, several examples of private networks have been established in the recent years. In **Spain**, for example, in 2019, Chinese provider Huawei partnered with Spanish operator Telefónica to build standard dedicated 5G at the Nou Camp football stadium in Barcelona, while, in 2020, German chemicals company BASF and Spanish telecommunications infrastructure vendor Cellnex signed an agreement to install the first 5G private network in the Spanish chemical industry. Within the automotive industry, instead, Volkswagen reported the start of the construction of its own 5G mobile networks in 122 factories in **Germany** in 2020 (EU 5G Observatory, 2021). A similar scenario concerns the Ford electric vehicle production site in Essex (**UK**), a project which also received state funding of £65 million from the UK government. Among non-EU countries, the UK in fact presents several examples of private networks, including

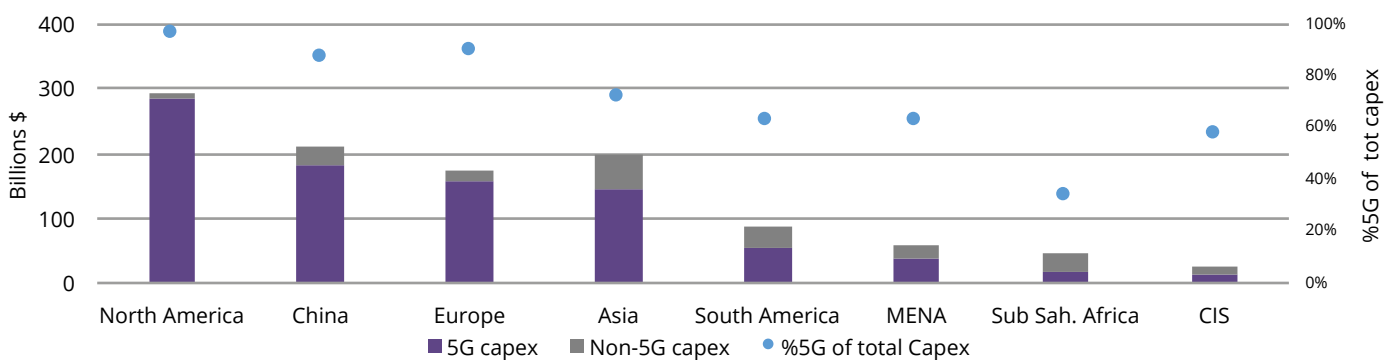
one installed by the high precision engineering company AE Aerospace. It was the first UK SME to deploy a 5G private network in collaboration with British operator BT, and was delivered thanks to a collaboration between Telefónica and Italy-based aerospace manufacturer Leonardo on private 5G for Industry 4.0 and aircraft systems as part of a joint defence project of the UK, Italy and Sweden.

1.5.3. Investments in 5G networks and perspectives of economic growth

Overall, data from the most recent years seems to suggest that the economic crisis triggered by the **Covid-19 pandemic has led to a slowdown in the progress of 5G networks**, both in infrastructural terms (for example, the delay in the implementation of base-station components and antenna mast systems) and in governmental and administrative terms, including the procedures concerning spectrum allocation[63]. Still, the ongoing crisis may well have played an **accelerating role in terms of the population's awareness** of the need for broadband and of the importance of advanced digital services, particularly in relation to telemedicine, e-health and teleworking. This could therefore have a **positive impact in the medium to long term** through an increase in demand, which could also have a significant effect on the acceleration of infrastructure development and deployment.

Fig. 1.5.11 5G investments worldwide (Bln $, 2021-2025)

Source: GSMA, Mobile Economy Report 2021



* The value for China includes Hong Kong, Macao, and Taiwan

63 In particular, auctions for frequencies in some countries have been delayed. This includes the French auction, which ended on 2 October 2020, reaching a total of 2,786 million for 310 MHz in the 3.4-3.8 GHz pioneer band.

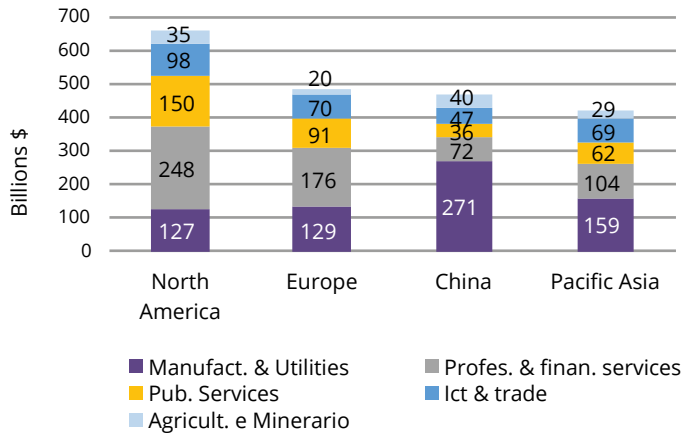
This is expected to have a lasting impact also on **investments** over the coming years, with financing from both government-run development programmes and the establishment of private networks. The GSMA forecasts that by 2025 a total of approximately **$900 billion** will be injected into transmission networks worldwide (Fig. 1.5.6), **80%** of which will be allocated to upgrading to the new 5G standard[64]. In particular, GSMA estimates almost $300 billion of investments in the US, about $200 billion in Asia, over $170 billion in Europe and more than $200 billion in China. In the latter two regions, the share of investments in 5G networks is expected to account for more than 85% of total investments in the whole telecommunications sector, while in North America, almost the entire amount of investments in such will be devoted to the new transmission standard. The worldwide scale of the 5G impact is also shown by the fact that substantial investments will also concern Latin America (around $80 bln) and MENA (Middle East and North Africa) ($60 bln). Finally, around $45 billion will be invested in Sub-Saharan Africa and around $25 billion in the Commonwealth of Independent States (CIS), thereby, **covering the whole world**.

According to GSMA estimates, investment in 5G networks, combined with their intensive use in both the private and public sectors, will **contribute $2.2 trillion to the global economy between 2024 and 2034** (Fig. 1.5.12). The major growth is expected to occur in the US (over $650 bln), followed by **Europe ($480 bln)** and China ($460 bln).

64 GSMA, Mobile Economy, June 2021.

Fig. 1.5.12 5G contribution to global economic growth by region and sector ($bln , 2034)

Source: GSMA, 2020



Where specific vertical market sectors are concerned, China could receive the largest benefits from the **manufacturing** and utilities sectors (up to $270 bln) while the **US and Europe should experience growth in revenues from professional and financial services** ($250 bln and $170 bln, respectively). It is also interesting to note that in terms of **public services,** Europe is likely to generate up to three times the benefits of China ($90 bln vs $30bln) but still significantly less than the US (around $150 bln).

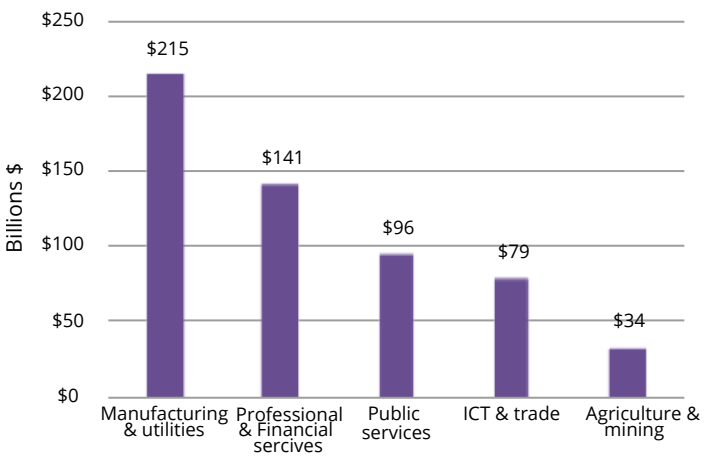
As 5G adoption increases and more users (both firms and individuals), and diverse services, migrate to fifth generation networks, spectrum across low, mid and high bands will be needed in order to deliver widespread coverage and enough capacity to support the delivery of 5G. A key role in this respect could be played by the **millimetre Wave bands** (24 GHz and above), which are

essential to satisfy high traffic demand at high network speeds while maintaining the performance and quality requirements of 5G services. The mmWave spectrum was internationally allocated to mobile services at the World Radio-communications Conference in November 2019 (WRC-19), with commercial mmWave 5G networks announced or launched in several countries, including Japan, Singapore and the US. The latter is one of the global leaders in the use of mmWave spectrum for 5G, with all major national operators already offering commercial 5G services using the band, while **Europe still lags behind**, with **only four countries having assigned the mmWave spectrum** to operators as of March 2021 (GSMA, 2021).

The use of **millimetre waves is expected to contribute $565 billion globally by 2034** (Fig. 1.5.13), with the largest benefits coming from the manufacturing and utilities sectors ($215 bln), professional and financial services ($141 bln) and public services ($96 bln).

Fig. 1.5.13 Economic impact of mmWave usage in 2034 at global level ($ bln)

Source: I-Com elaboration on GSMA (2020) data



1.5.4. The evolution of European connectivity targets: from the Digital Agenda for Europe to the Digital Decade. The initiatives to develop connectivity in Europe

Wide availability of high-performance networks is a prerequisite for citizens, businesses and public administrations to fully enjoy the benefits of digitalisation. The EU institutions, aware that the European Union is lagging behind other parts of the world, have set increasingly challenging connectivity targets and taken action in a range of areas to improve connectivity and define harmonised rules for connectivity services.

On 9 March 2021, the European Commission published the Communication ***"2030 Digital Compass: the European way for the Digital Decade"*** which is focused on four main areas representing the expression of digital sovereignty dimensions already described: secure and sustainable digital infrastructures, digital transformation of businesses, digital skills of citizens and digitalisation of public services. Considering that digialtisation can become – especially during the pandemic – a decisive enabler of rights and freedoms, allowing people to reach out beyond specific territories, social positions or community groups, and opening new possibilities to learn, have fun, work, explore and fulfil one's ambitions, the strategy set out a programme of policy reform, which has already begun with the Data Governance Act,

the Digital Services Act, the Digital Markets Act and the Cybersecurity Strategy (to be analysed in the following paragraphs).

For digital infrastructures, the strategy underlines the importance of ensuring an excellent and secure connectivity for everybody and everywhere in Europe and achieve gigabit connectivity by 2030. To this end, any technology mix can be used even if the focus should be on the more sustainable next generation fixed, mobile and satellite connectivity, with Very High-Capacity Networks including 5G being rolled out.

To guarantee the realization of the ambitions identified, the communication proposes a Digital Compass in the form of a policy programme to be adopted by the co-decision of the European Parliament and Council. This includes concrete targets, a governance structure with annual reporting by the Commission to the European Parliament and Council on the progress towards the Digital Decade, the monitoring of digital principles endorsed in the inter-institutional declaration and a mechanism to organise with MSs those Multi-Country Projects that are necessary for building Europe's digital transition in critical areas.

From the adoption of this strategy, several initiatives were launched by the Commission to encourage and accelerate the development of connectivity infrastructures.

Specifically, the **2018 European Electronic Communications Code** has updated the rules for radio spectrum management across the EU, calling for creating a stable and harmonised regulatory environment and facilitating innovation, particularly through 5G networks. The Code calls for long licence durations, coupled with clear rules on licence renewals and more stringent requirements to use spectrum effectively and efficiently, fixes strict deadlines for the use of pioneer spectrum bands for 5G, as well as for spectrum harmonised for wireless broadband networks and services, seeks to ensure better coordination of spectrum policies and assignment conditions across the EU, with a peer review mechanism, facilitates the deployment of 5G networks, provides more means for national authorities to support competition and creates an improved spectrum coordination mechanism. In view of a better implementation of 5G networks, the code invites MSs and European institutions to cooperate in order to implement policies of strategic planning, coordination and harmonisation of the use of radio spectrum. More specifically, the MSs must ensure its effective management by guaranteeing that its allocation, as well as the granting of the relative general authorisations and individual rights of use by the competent authorities, are based on objective, transparent, non-discriminatory and proportional criteria. Specifically, the granting of individual rights of use must be limited to situations where such rights are necessary to maximise the efficient use of spectrum in light of demand, and their duration must not be less than 20 years, which should ensure legal certainty and stimulate long-term investment.

In July 2020, the European Council agreed on the **Recovery and Resilience Facility**, the centrepiece

of NextGenerationEU, a temporary recovery instrument that allows the Commission to raise funds to help repair the immediate economic and social damage brought about by the coronavirus pandemic. In order to receive funds from the Facility, Member States must prepare national recovery and resilience plans of which at least 20% must be allocated in support of digital transformation. Amongst the flagship areas for investments and reforms, the roll-out of rapid broadband services is one of the most important.

To accelerate infrastructure development, in September 2020, the Commission adopted **Recommendation n. 2020/1307 on a common Union toolbox for reducing the cost of deploying very high-capacity networks and ensuring timely and investment-friendly access to 5G radio spectrum, to foster connectivity in support of economic recovery from the Covid-19 crisis in the Union**. The aim of the recommendation is for MSs to develop a toolbox of best practices for reducing the cost of deploying electronic communications networks and for efficient access to the 5G radio spectrum. This recommendation sets a deadline of 20 December 2020 for MSs to identify and share best practices, and a deadline of 30 March 2021 for MSs to finalise an agreement on the toolkit. Finally, the Commission set a deadline of 30 April 2021 for each MS to submit a roadmap for the implementation of the toolkit and a deadline of 30 April 2022 to report on the implementation of the toolkit.

In October 2020, the Connectivity Special Group, made up of MS representatives responsible for the area of electronic communications and the Commission was established to assist MSs in identifying and agreeing on the best practices and, upon request, in the implementation and reporting of the toolbox.

In line with the roadmap set out in the recommendation, MSs, in close cooperation with the Commission, agreed on 25 March 2021 on a **Connectivity Toolbox** outlining a set of best practices to reduce these costs, promote access to physical infrastructures and streamline authorisation procedures for civil works.

1.6. CYBERSECURITY

1.6.1. Cybersecurity in the EU. An overview

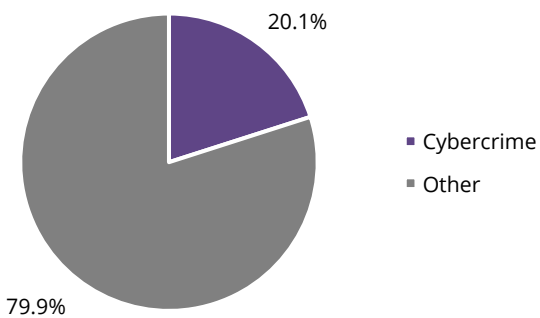
Over the last decade digitalisation has transformed everyday life. Digital platforms in recent years, and overall, during the Covid-19 pandemic, have represented the privileged space where individuals can carry out their work, social and leisure activities. According to the EU Commission, 40% of European workers have experienced forms of tele-work since the start of the pandemic, making home computers, which are generally less protected than office and company devices, the point of access to data and valuable digital activities. Together with many advantages (always accessible, everywhere and at any moment), this relatively new way of living has brought to light many new problems in terms of security and, specifically, cybersecurity.

The digital environment is vast and, therefore, an ideal ground for cyberattacks that can be either indiscriminate or targeted, aimed at large and small organisations in both the public and private sectors. Therefore, Internet usage and its connected devices offer new opportunities for people and companies but, at the same time, create new risks. The range of potential attacks and attackers is wide and becoming more so by the day, up to the point that at the Davos World Economic Forum of 2021 cybersecurity was regarded as one of the greatest economic risks for the ongoing year. The new technologies, mobiles, smart devices connected to the Internet of Things and many AI applications expose both private and public organisations to attackers, increasing the risks of, for example, shutdowns or subversion of industrial control systems. Furthermore, attacks are becoming worryingly more sophisticated and costly to detect.

The dimensions that this problem has assumed are even more evident by observing the data contained in the latest version of the summary report "Europol in Brief". The European agency that supports and coordinates the national authorities of the various MSs in combating serious forms of transnational crime in 2019 focused 20.1% of its total operations on the fight against cybercrime (Fig. 1.6.1). So, one in five supranational crimes is a cybercrime. According to a study carried out by Comparitech **in the third quarter of 2019, 9.68% of computers and 3.04% of mobile devices in the EU were infected with malware**[65]. Comparing the European data with

Fig. 1.6.1 Europol operations, by type of crime (2019)

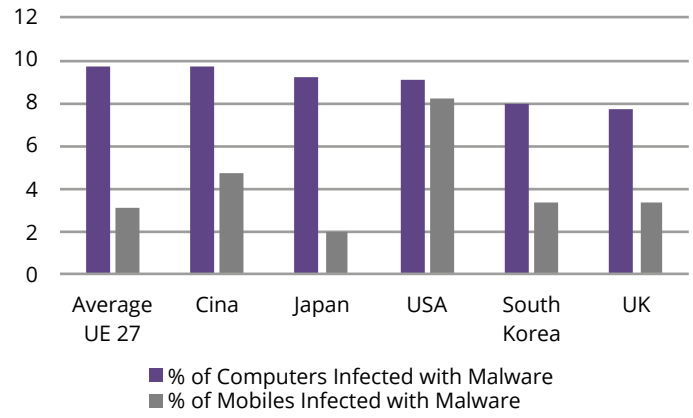
Source: Europol in brief 2019



65 Malware is any software intentionally designed to cause damage to a computer, server, client or computer network

Fig. 1.6.2 Cyberattack target devices, by geographical area (2019)

Source: Comparitech, 2020



those of the other major world economies, we can see how the EU ranks first for the percentage of infected computers, ahead of China, Japan, the USA, South Korea and the UK. Instead, where mobile devices are concerned, the EU MSs are on average more protected than those of all the other geographical areas considered except for Japan (Fig.1.6.2). By observing the individual EU MSs (Fig.1.6.3), we can see that those most targeted by cyberattacks on computers are France (15.09%) and Greece (14.59%). Instead, those most vulnerable on mobile devices are Romania (5.04%) and Italy (5.01%).

The latest version of the CLUSIT Cybersecurity Report, which annually considers cyberattacks classified as

Fig. 1.6.3 Cyberattack target devices in the EU (2019)

Source: Comparitech, 2020

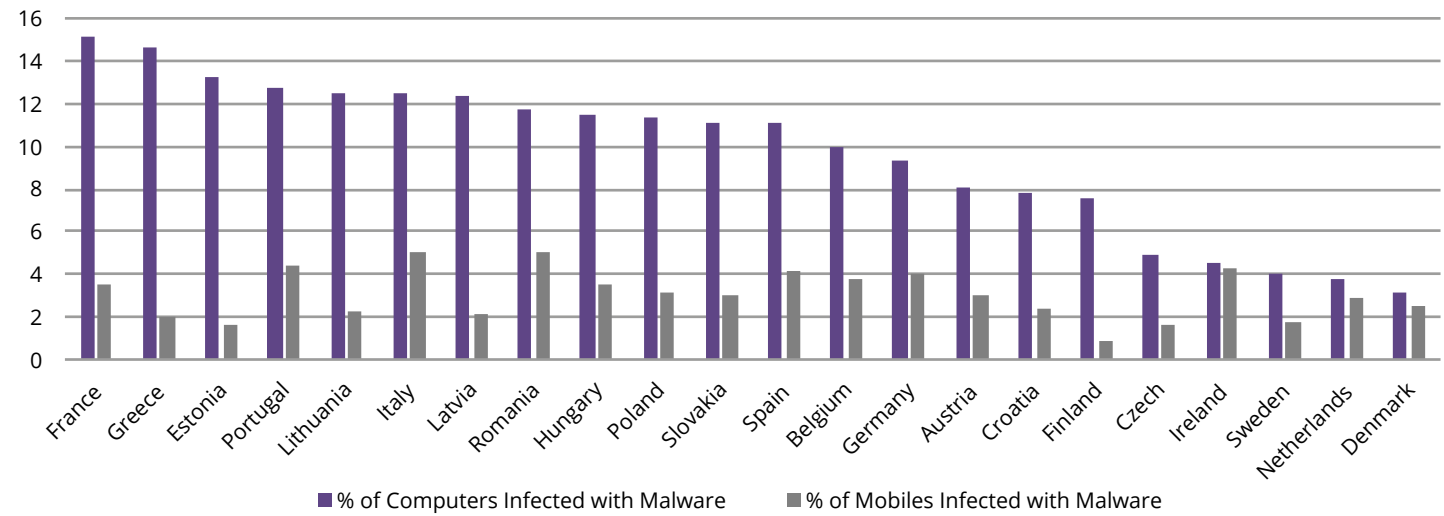


Fig. 1.6.4 Serious cyberattacks globally (2020)

Source: Clusit

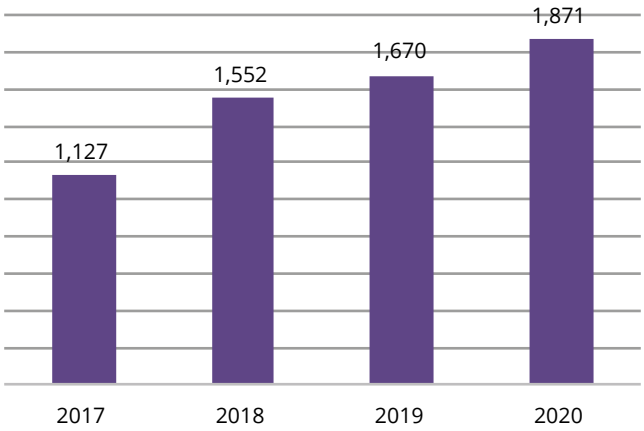
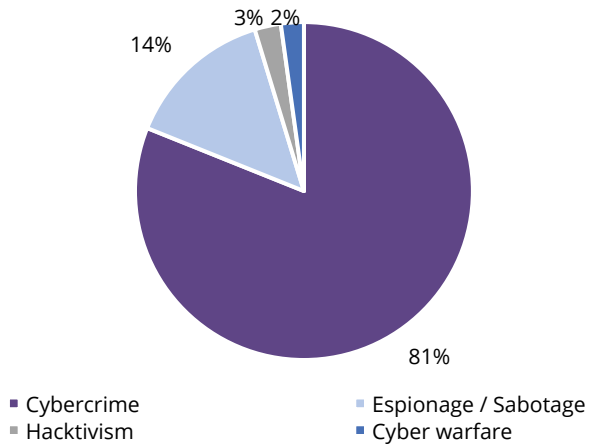


Fig. 1.6.5 Reasons behind serious cyberattacks (2020)

Source: Clusit



serious[66] globally, in 2020, detected 1,871 cyberattacks, with a significant increase compared to the 1,670 attacks recorded in 2019 and the 1,552 recorded in 2018. Observing the trend of serious attacks recorded in the last 4 years, it is possible to note that between 2017 and 2020 the number of particularly significant actions increased by 40%, 11% being only in the last year (Fig. 1.6.4).

As for the reasons behind these serious cyberattacks (Fig. 1.6.5), Clusit classifies these episodes for 81% of cases in the Cybercrime category, i.e., aimed mainly at obtaining an economic profit through stolen data. The second most important category is Espionage / Sabotage which would seem to motivate 14% of the serious malicious actions that took place in 2020. All the espionage and sabotage activities carried out using illicit computer techniques are attributable to this category. Less relevant are malicious actions motivated by political or social purposes (Hacktivism) and those carried out in the context of cyber warfare (the set of techniques for collecting, processing, managing, disseminating information to obtain an advantage in the military, political or economic field).

For organisations, suffering a cyberattack that involves the loss of data generates a negative impact of extreme importance both from the economic point of view and on the loss of trust on the part of users. The latest version of the "Cost of a Data Breach Report" study, conducted by IBM, tried to estimate the average cost of a data breach that falls on the companies

66 Serious attacks are those that have reached a level such as to become public domain, or with a systemic impact on every aspect of society, politics, economics and geopolitics.

Fig. 1.6.6 Average cost of a data breach, by country ($ mln)

Source: IBM

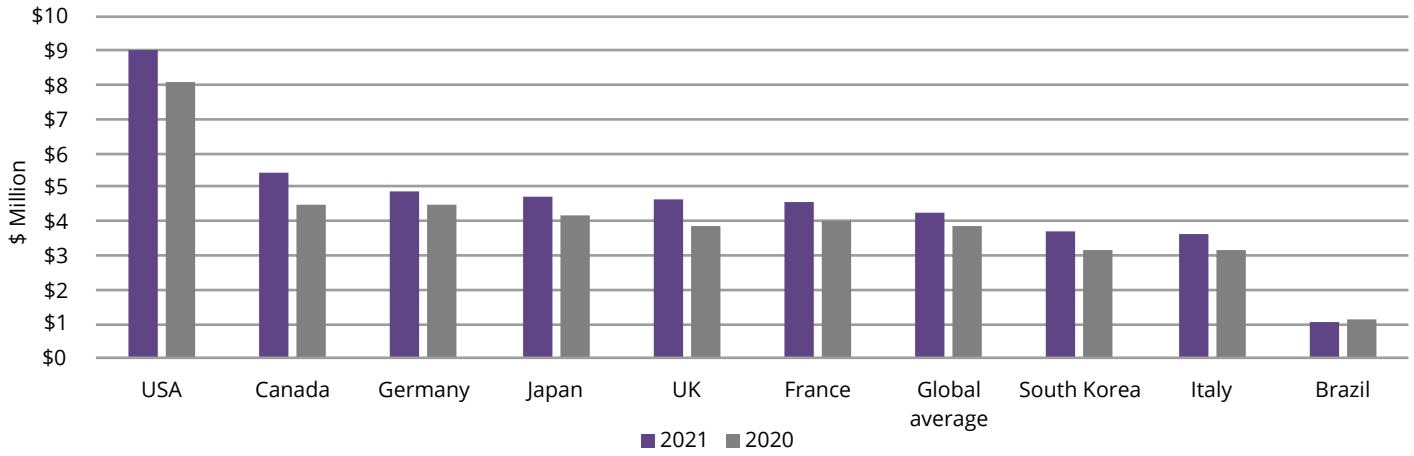
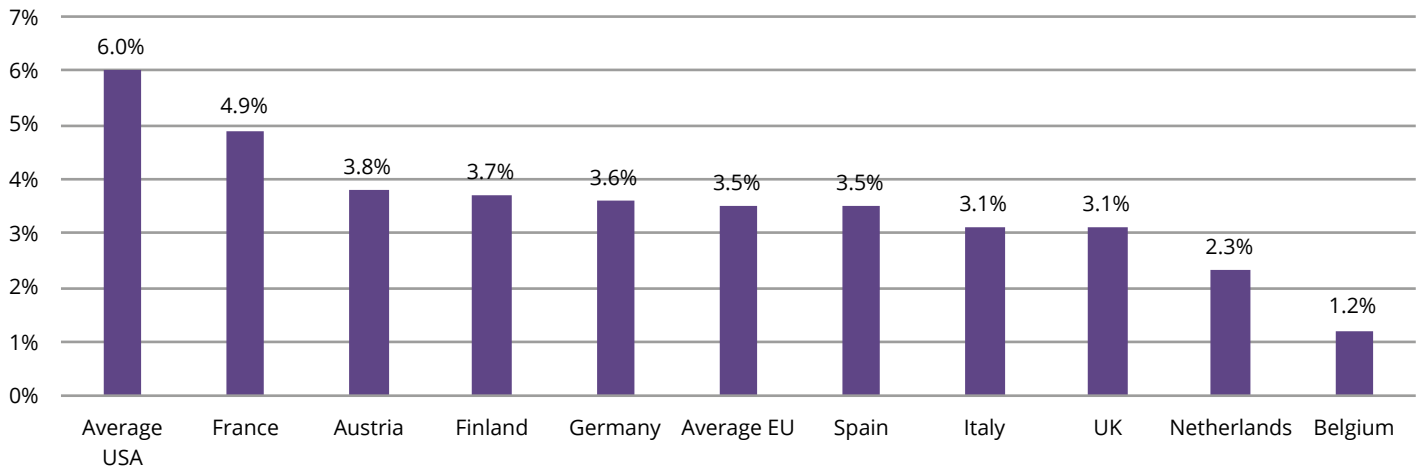


Fig. 1.6.7 IT security spending by organisations as a share of total IT budget, by geographic area (%)

Source: ENISA, 12-2020



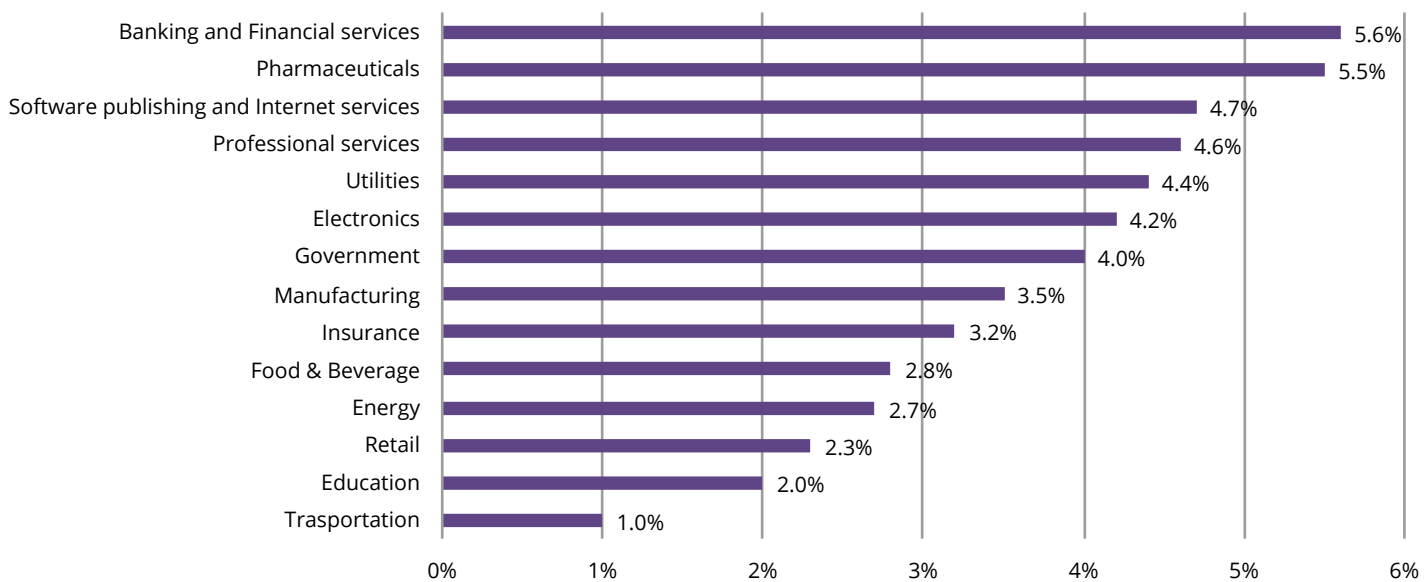
that are victims of it. During the analysis, conducted by interviewing 3,500 representatives of the organisations involved, 537 violations occurring in 17 different countries were examined. According to the study, the average cost of violations globally is estimated to be around $4.2 million in 2021. By observing the time trend, it is possible to see how the economic repercussions on companies affected by cyberattacks have grown by 15% between 2017 (the year they amounted to $3.62 mln) and 2021, 9% being only in the last year (Fig.1.6.6).

This data highlights the need to increase investments in IT security. **The "NIS Investments" report released by ENISA in December 2020 shows how the average IT security spending of European organisations (in relation to the IT budget) is considerably lower than the average for US organisations.** Looking at data released by ENISA (Fig.1.6.7), we can see that among European countries, the French organisations allocate the largest share of their IT budget to security.

The average budget invested by businesses for NIS Directive implementation projects is approximately €175,000, with 42.7% of affected organisations allocating between €100,000 and €250,000. The sectors in which the largest share of the IT security budget is invested

Fig. 1.6.8 IT security spending by organisation as a share of total IT budget, by industry (%)

Source: ENISA, 12-2020



(Fig.1.6.8) are in banking and financial services (5.6%), pharmaceuticals (5.5%) and software publishing and Internet services (4.7%).

The sectors registering the worst performance are also two of the most important, education (2%) and transport (1%). Transport, in particular, with the spread of self-driving vehicles, could become increasingly targeted by cybercriminal attacks. The Commission is very aware of the need for further investments in the sector. For the detection and the deterrence of cybercrimes, the Commission has launched the Cybersecurity Competence Centre in Bucharest. Further investment opportunities are now expected from the MSs thanks to the EU Recovery Fund plan.

1.6.2. The European regulatory framework on cybersecurity

The digital transformation of society and the economy has led to the rise of new security issues. Since 2013, the EU has worked on a wide legislation on cybersecurity to appropriately face the challenges of digitalisation. The EU Cybersecurity Strategy of 2013 was adopted to safeguard the online environment

providing security and freedom. It outlines the EU's vision and proposes actions aimed at pursuing cyber resilience, reducing cybercrime, developing an EU Cyber Defence Policy and fostering the industrial and technological resources required to benefit from the Digital Single Market.

Nevertheless, a significant step forward in the EU legislation on cybersecurity was represented by the **Directive on Security of Network and Information System** (the **NIS Directive**), adopted by the European Parliament on **6 July 2016**, entering into force in August 2016. MSs had to transpose the directive into national law by May 2018, following art. 7 of the directive itself, that explicitly identifies the leading principle for national strategies. Moreover, the directive encourages cooperation and the exchange of information among MSs by setting up a cooperation group made up of MS representatives, the European Commission and the EU Agency for Cybersecurity (ENISA). The group is involved in the planning, guidance, signaling and sharing of the strategies. In addition, the directive creates a network of agents active on security issues and identifies the security and notification requirements needed by digital service providers.

On 29 January 2020, the European Commission's new work programme was published and under the second priority, "A Europe fit for the digital age", the Commission announced its intention to launch a review of the Directive on Security of Network and Information Systems (NIS Directive), in order to 'further strengthen overall cybersecurity in the Union'.

Consequently, on **25 June 2020**, the Commission launched the **public consultation for the revision of Directive 2016/1148** on measures for an EU common level of network and information systems security ("NIS Directive"). The launch of the public consultation (closed on 2 October) was in line with the periodic review of the NIS Directive, provided for in art. 23, to verify its functioning and application in the individual

MSs. The review had to take place, as announced by the Commission and in line with the political objective of making "Europe fit for the digital age", by the end of 2020 prior to the May 2021 deadline set by the afore-mentioned article. On **16 December 2020,** a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive) was published (this proposal is part of a package that also includes a proposal for the directive on the resilience of critical entities and the new Cybersecurity Strategy as explained in more detail below). The proposal, specifically: a) expands the scope of the current NIS Directive by adding **new sectors** based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope; b) leaves some flexibility for MSs to identify smaller entities with a high security risk profile and **eliminates the distinction between operators of essential services and digital service providers**. Entities would be classified based on their importance and divided respectively into essential and important categories with the consequence of being subjected to different supervisory regimes; c) **strengthens security requirements for the companies**, by imposing a risk management approach providing a minimum list of basic security elements that have to be applied and introducing more precise provisions on the process for incident reporting, content of the reports and timelines; d) sets **more stringent supervisory measures for national authorities**, stricter enforcement requirements and aims at harmonising sanctions regimes across MSs; e) enhances the **role of the Cooperation Group** in shaping strategic policy decisions on emerging technologies and new trends; f) increases **information sharing and cooperation** between MS authorities and enhances operational cooperation including on cyber crisis management; g) stablishes a **basic framework with responsible key actors** on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creating an EU registry on that operated by the European Union Agency for Cybersecurity (ENISA).

With **Regulation 2019/881**, known as the **Cybersecurity Act**, the EU reached a political agreement to strengthen the EU Agency for Cybersecurity (**ENISA**) and established a wide certification framework on digital products, services and processes. The first part of the regulation, specifically the first 45 articles, disciplines the mandate, resources and new tasks of the ENISA, while from art. 46 on, it describes the certification framework for cybersecurity with the aim of building up a Single Digital Market. The ENISA must propose implementation acts that the Commission can adopt, and it must also evaluate each certification system every 5 years. The regulation identifies a set of security requirements for the European certification systems, dividing them into three groups – basic, substantial and high – and basing the evaluation on the expected risk level associated with the use of the product, service or process in terms of impact and probability of the occurrence of product inconvenience and liability. It specifies the evaluation activities and the remedies for each category. Furthermore, it prescribes

at the organisational level the identification of a national authority in each Member State.

In addition, the Cybersecurity Act establishes the **European Cybersecurity Certification Group** (ECCG), made up of representatives from national cybersecurity certification authorities or other relevant national authorities, to assist the Commission in its work to ensure the implementation and application of the act, being an advisor in the relations between the Commission and the ENISA.

By 28 June 2024, and then every 5 years, the Commission will have to evaluate the impact and effectiveness of the ENISA and its work, with the possibility to modify its mandate and subsequent financial implications.

On **16 December 2020**, the Commission launched several initiatives on security. Specifically, the Commission adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive) already analysed above, a proposal for a Directive on the Resilience of Critical Entities (2020/0365 (COD) and the new Cybersecurity Strategy.

As a part of the Recovery Plan Communication, "*Europe's moment: Repair and Prepare for the Next Generation*", the Commission published a **new Cybersecurity Strategy**. Starting from the consideration that transport, energy and health, telecommunications, finance, security, democratic processes, space and defence are heavily reliant on networks, information systems are increasingly interconnected and these cross-sector interdependences increase vulnerabilities to cyberattacks, the Commission has launched a strategy focused on three pillars and connected initiatives: **1) resilience, technological sovereignty and leadership**. To achieve these goals the Commission proposes: a) the reform of EU rules on the security of Network and Information Systems (launched on the same data of new Cybersecurity Strategy); b) the constitution of **network of Security Operations Centres** across the EU and the support to the improvement of existing centres and the establishment of new ones to create collective knowledge and share best practices also supporting the training and skill development of staff operating these centres: c) the deployment – in 2021-2027 – of **a secure quantum communication infrastructure (QCI)** for Europe able to offer public authorities a brand new way to transmit confidential information using an ultra-secure form of encryption to shield against cyberattacks, built with European technology; d) the adoption, under the Cybersecurity Act, of the **first Union Rolling Work Programme** in the first quarter of 2021 (to be updated at least once every three years) to incentivise safe products and services without compromising on performance and allow industry, national authorities and standardisation bodies to prepare in advance for future European cybersecurity certification schemes. The Commission also announces the will to consider a comprehensive approach, including possible new horizontal rules to improve the cybersecurity of all connected products and associated services placed on the Internal Market; e) the development of a **contingency plan**, supported by EU funding, for dealing with extreme scenarios affecting the integrity and availability of the global DNS root system; f) the support for the adoption of a **DNS resolution**

diversification strategy, the development of a **public European DNS resolver service** and **the uptake of key Internetstandards**includingIPv664andwell-established Internet security standards and good practices for DNS, routing, and email security; g) the development of a dedicated **cybersecurity Masters programme**, and the definition of a **common European Cybersecurity Research and Innovation Roadmap** beyond 2020; h) the upskilling of the workforce, the development, attraction and retention of the best cybersecurity talent and investments in world class research and innovation. **2) building operational capacity to prevent, deter and respond.** The Commission identifies several strategic initiatives to be implemented and specifically: a) complete the **European Cybersecurity Crisis Management Framework** and determine the process, milestones and timeline for establishing the Joint Cyber Unit; b) continue implementation of **cybercrime agenda** under the Security Union Strategy; c) encourage and facilitate the establishment of a MS **cyber intelligence working group** residing within the EU INTCEN; d) advance the EU's **cyber deterrence posture** to prevent, discourage, deter and respond to malicious cyber activities; e) review the **Cyber Defence Policy Framework**; f) facilitate the development of an EU "**Military Vision and Strategy on Cyberspace as a Domain of Operations"** for CSDP military missions and operations; g) support **synergies** between civil, defence and space industries; h) reinforce cybersecurity of critical space infrastructures under the Space Programme. **3) advance a global and open cyberspace.** To this end, the Commission underlines that the EU should: a) define a set of **objectives in international standardisation processes**, and promote these at international level; b) advance international security and stability in cyberspace, notably through the proposal by the EU and its MSs for a **Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA)** in the United Nations; c) offer practical guidance on the application of **human rights and fundamental freedoms in cyberspace**; d) better **protect children** against child sexual abuse and exploitation, as well as a Strategy on the Rights of the Child; d) strengthen and promote the **Budapest Convention on Cybercrime**, including through the work on the Second Additional Protocol to the Budapest Convention; e) expand EU **cyber dialogue with third countries**, **regional and international organisations**, including through an informal EU Cyber Diplomacy Network; f) reinforce the **exchanges with the multi-stakeholder community**, notably by regular and structured exchanges with the private sector, academia and civil society; g) propose an EU **External Cyber Capacity Building Agenda** and an **EU Cyber Capacity Building Board**.

The strategy also underlines the importance to improve the overall level of cybersecurity through consistent and homogeneous rules announcing proposals for common binding rules on information security and for common binding rules on cybersecurity for all EU institutions, bodies and agencies in 2021, based on ongoing EU inter-institutional discussions on cybersecurity.

In this context, the institution of the **European**

Cybersecurity Competence Center (ECCC) in Bucharest is crucial to bring together various organisations from industry, academia and civil society to create a so-called cybersecurity skills community and collaborate with a network of national coordination centres.

Within this set of initiatives, there is also the adoption of the **Next Generation EU** which will allow the Commission to contract, on behalf of the Union, loans on the capital markets of up to €750 billion at 2018 prices with the EU commitment to use the loans contracted on the capital markets for the sole purpose of dealing with the consequences of the Covid-19 and which identifies cybersecurity as one of its top priorities, in accordance with the position expressed by the Council on 9 June 2020. This was especially linked to the increased cyberattacks occurring during the lockdown, showing the vulnerability in the current IT system. Over the last weeks, there has been an extraordinary increase in malicious attacks from multiple sources, attempting to capitalise on the sudden digital disruption caused by the pandemic (millions of digitally unskilled people were obliged to carry out activities on the Internet, being exposed to threats). Furthermore, the crisis has also shown the need for a stronger industrial and technological presence in strategic parts of the digital supply chain, since the security of technology is emerging as a critical and central key-topic.

As well as the reinforcements financed under NextGenerationEU, other programmes are focusing on making the Union more resilient and addressing challenges that have been heightened by the pandemic and its consequences. These include boosting the Union's cyber-defences and supporting the digital transition by equipping the **Digital Europe Programme** with a total budget of €8.2 billion.

1.6.2.1. 5G and security

The continually evolving digital environment requires the European system to be able to define and implement effective security standards in order to make the development of 5G networks possible. This is a core target as these networks are a key element for the internal market to evolve, especially for the effective management of core economic and social services, such as energy, transport, financial services, health systems and industrial controls.

On 26 March 2019, the Commission adopted **Recommendation 2019/534** on the cybersecurity of 5G networks, highlighting the risks for these networks and suggesting risk-analysis and management methods at the national level to be implemented within a coherent European context. For 5G networks, it identifies a clear roadmap that the MSs must follow to evaluate risks, updating the requirements for firms that provide public communication networks or public communication services. In order to achieve an effective prevention of and fight against threats, the document points out the importance of a **European coordination of the evaluation systems** and encourages **information sharing between MSs and the European institutions**, in order to reach a common awareness of the cybersecurity risks connected to 5G networks. Moreover, each MS

should have communicated its national evaluations to the ENISA by 15 July 2019, in order to complete a specific map of the 5G environment in Europe. Finally, the recommendation encouraged MSs to cooperate with the Commission in evaluating the effects of the document itself by 10 October 2020.

Hence, consistent with the recommendation, the **NIS Cooperation Group** has published a **EU-wide coordinated risk assessment of 5G network security**. This is a report that, starting from the respective MS's evaluations, identifies the most important threats and most dangerous agents, the sensitive resources, the main vulnerabilities and the different strategic dangers. The report also focuses on the innovations brought about by these networks and, as well, the role of providers in setting up and using 5G networks, and the degree of dependence from the single provider. It also stresses the importance of the implementation of a new security paradigm through the analysis of the current strategic framework. Moreover, in its conclusions on 3 December 2019, the Council sustained the remarks of the Cooperation Group, once again underlining the importance of a coherent approach to avoid market fragmentation.

On 29 January 2020, the Commission published the **Communication "Secure 5G deployment in the EU – Implementing the EU toolbox"** which took note of the absolute importance of 5G for many essential services and, therefore, the strategic need for the Union to ensure 5G network cybersecurity at a time when cyberattacks are both on the rise, more sophisticated and affecting a wide range of stakeholders. Under the NIS cooperation and following the completion of MSs' 5g network infrastructure risk assessment procedures, the NIS Cooperation Group published a EU-wide report on the coordinated cybersecurity risk assessment of these networks, identifying the most important threats and their main perpetrators, the most sensitive resources and major vulnerabilities (technical and other) affecting 5G networks.

On the same date, the NIS Cooperation Group published the EU's **package of instruments**, including risk mitigation measures. It deals with all the risks identified in the coordinated risk assessment report, identifying and describing a range of strategic and technical measures, as well as corresponding support actions aimed at strengthening their effectiveness, which can be implemented to mitigate the identified risks. The document, in highlighting how Europe is one of the most advanced regions in the world regarding the commercial launch of 5G services (by the end of 2020, the first 5G services should have been available in 138 European cities), takes stock of some of the areas where 5G will operate as an enabling factor for a number of important applications and, more specifically, in e-health, intelligent energy networks, future factories, media and entertainment and mobility.

The document's objective was to identify a possible common set of measures to **mitigate the main cybersecurity risks of 5G networks** (as identified in the EU-coordinated risk assessment report) and to provide **guidance in selecting the measures to be taken** so

as to create a robust framework ensuring an adequate level of cybersecurity in the 5G networks across the EU and a coordinated MS approach.

The package's measures will contribute to achieving a number of important **safety objectives** necessary to address the risks identified in the risk assessment report and to protect the confidentiality, integrity and availability of 5G networks. These objectives are based on: a) strengthening security in the design, implementation and operation of networks; b) raising **basic safety standards** for product and service safety; c) minimising **exposure to the risks** arising from the risk profile of individual suppliers; d) avoiding or limiting the **main dependencies on a single provider** in 5G networks; and e) promoting a **diverse, competitive and sustainable market for 5G equipment**. The **package** identifies **8 strategic measures** and **11 technical measures** which are to be supported by a **number of actions** based on reviewing or developing network security guidelines and best practices, strengthening the testing and control capabilities at a national and European level, supporting standardisation, exchanging best practices on the implementation of strategic measures (especially, national disciplines for assessing the risk profile of suppliers), ensuring that public-funded 5G implementation projects take into account cybersecurity risks and ensuring the application of standard technical and organisational security measures through a specific European Certification Scheme. Paragraph 4.2 identifies **risk mitigation plans** for each of the nine risk areas identified in the EU-wide coordinated risk assessment report. These involve a combination of strategic and/or technical measures (along with appropriate support actions) that are classified into four levels, based on an assessment that considers risks to be faced and the persistent risks occurring after the application of the same measure. In conclusion, the toolbox calls on MSs to implement measures and obtain the necessary powers to mitigate risks, by strengthening security requirements for mobile network operators, assessing the risk profile of suppliers, and applying appropriate restrictions on suppliers considered to be high risk. The latter includes the necessary exclusions for critical assets, ensuring that each operator has an adequate multi-supplier strategy to avoid or limit any heavy dependence on a single supplier and avoid dependence on suppliers. The Commission expressed its willingness to continue to provide full support and take all relevant actions within its powers in order to support MS implementation of the package of instruments and to strengthen its impact.

On **24 July 2020**, the NIS Cooperation Group, with the support of the Commission and ENISA, published a **report on MSs' progress in implementing the 5G security toolbox**. It takes stock of the level of maturity reached by the various countries in the implementation of the measures contained in the toolbox and shows how, although all MSs have started to revise and strengthen their security measures in view of 5G, in some countries this work is still ongoing and, therefore, no final measures have yet been taken. At a general level, the report highlights that the three main risks identified are the incorrect configuration of networks,

the lack of access control and state interference through the 5G supply chain. Regarding the latter, it highlights the belief, widespread among states, in the lack of adequate existing measures. Where the dependence on individual suppliers is concerned, the report highlights the need to understand the involvement of different suppliers in the individual elements of the network, the technical and operational difficulty of applying a multi-vendor strategy at certain points of the network, the limited number of 5G suppliers, the major critical issues for smaller countries, the possible effects on operators resulting from the formulation of diversified requests to suppliers and the need to identify specific regulatory bases that allow for imposing certain obligations on suppliers. Also interesting, are the considerations related to the implementation of measures to ensure the security of 5G networks. On this specific point, the document, after having defined the medium-low level of maturity reached in the implementation of such measures, describes a rather diversified panorama where, however, the request emerges from many MSs for a coordinated approach to EU standards. The deadline for MSs, in cooperation with the Commission, to determine whether further action is needed, expired on 1 October 2020.

On 16 December 2020, with the support of EU Member States and ENISA, the EU Agency for Cybersecurity, the Commission published a **report analysing the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks and the progress made in implementing the EU toolbox of mitigating measures since the progress report of July 2020**. As a result of its review of the recommendation, the Commission found that most MSs were well on track to implement a significant part of the measures recommended in the toolbox in the near future. Going forward, the Commission called on MSs to complete the implementation of these measures by the second quarter of 2021 and to ensure that identified risks had adequately been mitigated and in a coordinated way, in particular with a view to minimising the exposure to high-risk suppliers and of avoiding dependency on these suppliers.

In February 2021, European Commission tasked Enisa, the EU cybersecurity agency, with developing a **5G certification system** that would help address risks related to technical vulnerabilities in networks. To this end, ENISA launched a call for tender – closed on 30 June 2021 – to set up a working group to prepare a new 5G certification scheme.

PART 2 HEALTH

2. HEALTH

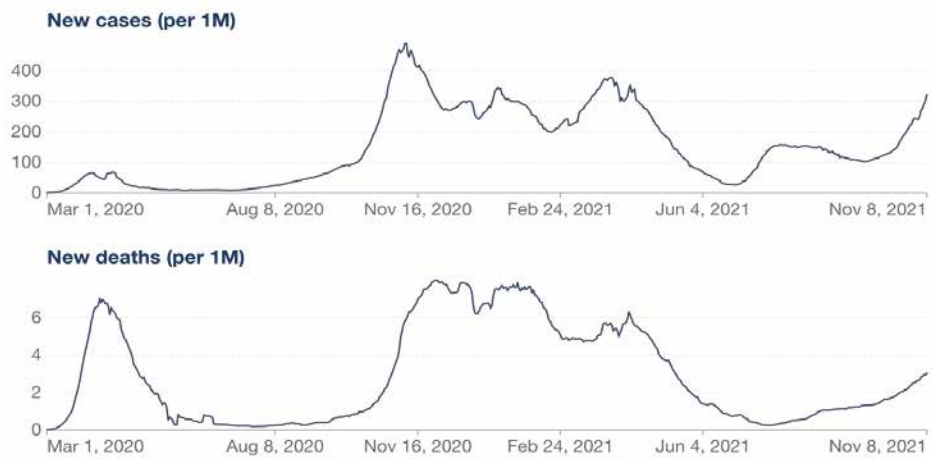
2.1. THE EUROPEAN PUBLIC HEALTH RESPONSE TO THE CORONAVIRUS PANDEMIC

2.1.1. Covid-19 in Europe. First outbreak and current situation

The Covid-19 pandemic continues to pose a major public health threat to EU/EEA[67] countries and the UK. The first official cases occurred at the end of January 2020, peaking for the first time in early April 2020 in the EU/EEA, with many countries implementing a range of response measures which led to a reduction in cases. **As countries regained control of transmission and alleviated the burden on healthcare, many measures were relaxed or removed to allow for a more viable way of life with the virus in circulation**. Subsequently, another increase in Covid-19 cases was reported in many countries (Fig. 2.1.1) leading to the beginning of the "second wave" in October 2020. After the peak in November, the number of cases kept fluctuating, reaching another peak in April 2021 and decreasing during the last summer. **From January 2021, the delivery of the Covid-19 vaccines and the vaccination campaigns carried out by every MS led to a progressive decrease in the case fatality rate.** However, once again, the number of cases is following a growing trend and it is likely we are at the beginning of another wave.

Fig. 2.1.1 Daily new confirmed Covid-19 cases and deaths per million people (7-days rolling average)

Source: Johns Hopkins University CSSE Covid-19 Data

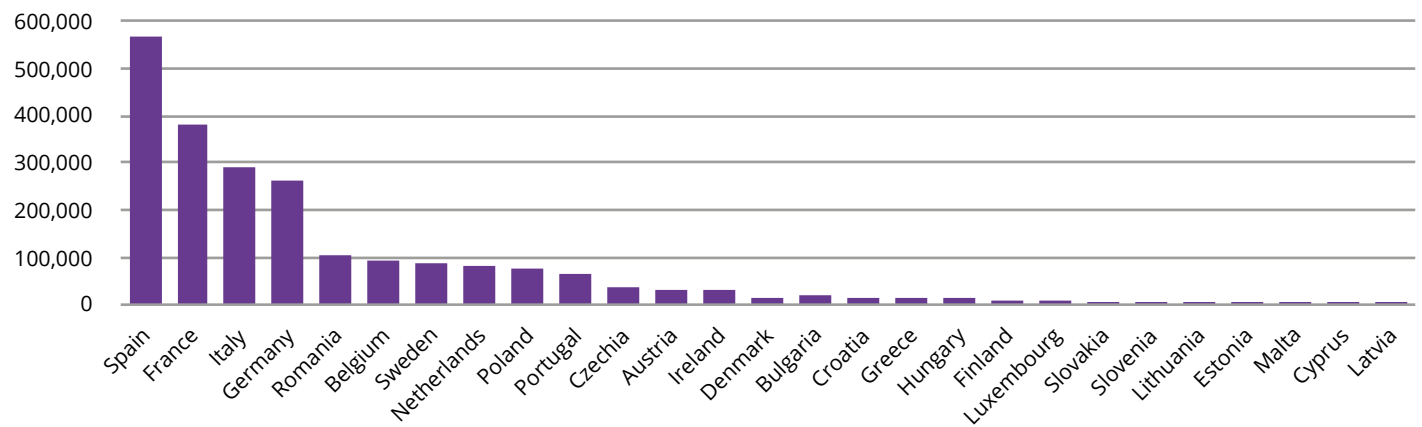


67 The EEA includes EU countries and also Iceland, Liechtenstein and Norway. It allows them to be part of the EU's single market.

In order to better understand the role that the EU should play in such a situation, it is crucial to analyse the first responses of each MS when the virus started spreading. Figure 2.1.2 shows current differences in Covid-19 cumulative case numbers among the EU-27 countries (UK not included), while Figure 2.1.3 shows the cumulative number of Covid-19 cases per 1 million inhabitants. Both graphs take into account the first wave of cases, i.e. the period from the first cases to September 2020. **During the summer of 2020 the first signals of a new increase in the number of cases were already confirmed in a number of EU countries**, mainly in Spain and France, where the incidence was 270 cases per 100,000 inhabitants and 153 cases per 100,000 inhabitants, respectively. The risk assessment on Covid-19 published by the ECDC (on 10 August 2020) compares weeks 29/30 with weeks 30/31 of 2020, and reveals an increasing trend in the 14-day incidence of reported cases/100,000 population across and within countries[68]. All countries that reported an increased 14-day case notification rate also had increased testing rates per 100,000 population. Generally speaking, the age distribution was different when comparing the periods of January – May and June – July 2020. Between January and May 2020, 40% of cases were aged 60 years or above and the largest proportion of cases was reported among 50 – 59 year olds. Instead, in June

Fig. 2.1.2 Sum of Covid-19 cases in EU-27 countries since the beginning of the pandemic (until 14 September 2020)

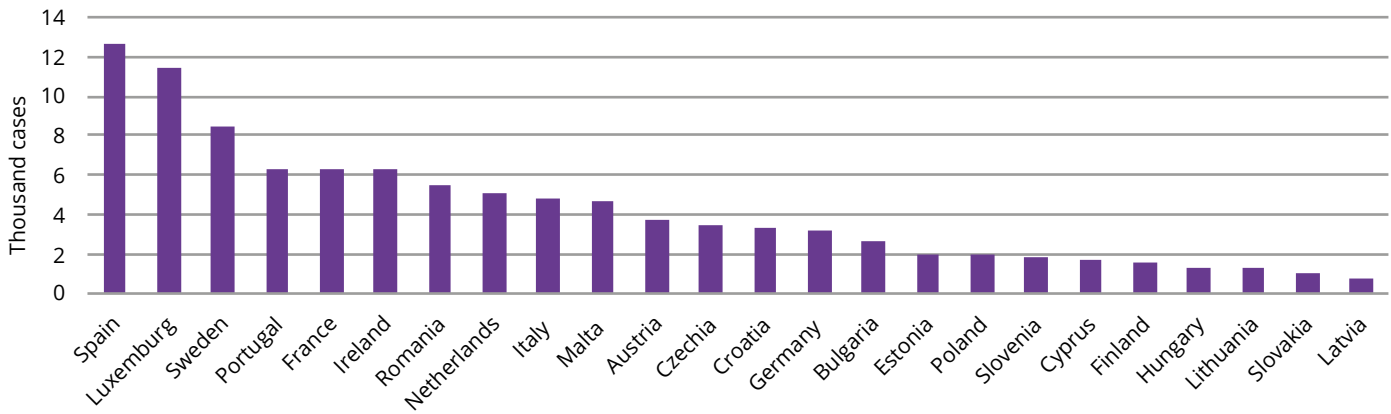
Source: ECDC



68 ECDC, Rapid risk assessment, Coronavirus disease 2019 (COVID-19) in the EU/EEA and the UK – eleventh update: resurgence of cases 10 August 2020

Fig. 2.1.3 Cumulative confirmed Covid-19 cases per million people (until 14 September 2020)

Source: Johns Hopkins University CSSE Covid-19 Data



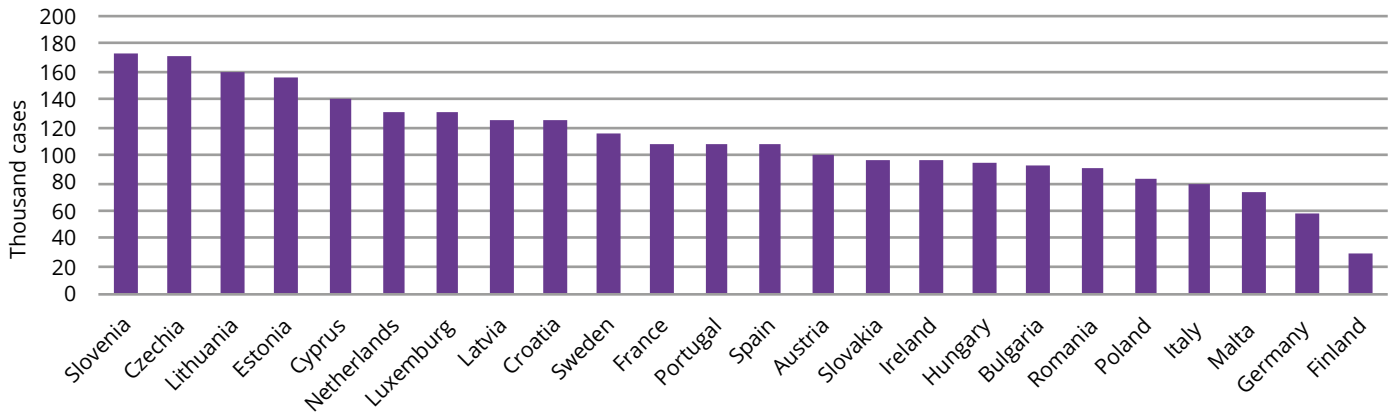
and July, people aged 60 years or above accounted for 17.3% of cases and the largest proportion of cases was reported among 20-29 year olds.

Comparing the data for the first wave to Figure 2.1.4 (data referring to the whole pandemic period), Eastern European countries struggled in containing the spread of the virus in the subsequent waves. However, the countries that reported a high number of cases in relation to the population in the first wave are still very affected today, such as Spain, Sweden, France, Portugal and the Netherlands.

During the first wave of cases, most European countries introduced multiple response measures, ranging from advice regarding hand and respiratory hygiene to limiting the size of non-essential groups to under 50 people, stay-at-home recommendations for risk groups, public space closures, and the mandatory and voluntary use of masks in the community, boarder closures and controls. Between 1 June and 1 July 2020, more than a half of the European countries (15 out of 31 EU/EEA and the UK) reduced the number of measures, while 2 out of 31 countries introduced additional measures to help control the spread of the virus. Since the beginning of the pandemic, contact tracing has been a key public health tool for the containment of Covid-19 clusters and outbreaks and is still ongoing across Europe, although implementation varies for time, and for regions and countries. There is no doubt that **health data and digital tools play a key role in this context and their employment is crucial in facing the emergency and for the quick response to the potential future crises**.

Fig. 2.1.4 Cumulative confirmed Covid-19 cases per million people (until 9 November 2021)

Source: Johns Hopkins University CSSE Covid-19 Data



2.1.2. The EU role in the response to the coronavirus outbreak

When the initial spread of the then novel coronavirus rapidly escalated, with the WHO designating the virus as a pandemic just a few months after its initial outbreak, the EU struggled to play a coordinating role, complementing national policies to help countries in facing common challenges – lack of sufficient healthcare organisation and provision – so that each Member State would be better prepared to face and respond to the virus. **While most federal states already had an authority or an agency with such a remit, and responsibilities on global health and epidemic intelligence, the equivalent did not exist for the EU at that time**. In the EU, responsibilities are decentralised to MSs, and they only began sharing information after the European Centre for Disease Prevention and Control (ECDC) was established in 2005. It is an EU agency aimed at strengthening Europe's defences against infectious diseases, and was mainly created in response to the SARS outbreak in order to coordinate a European response to future outbreaks[69]. However, it has a limited function and does not engage in public health decision making. The European health policy relies on three EU pillars: the first is Article 168 of the Treaty on the functioning of the European Union (TFEU) which gives the EU a role in health security, including (at that time) two agencies – the ECDC and the drugs agency (OEDT) – which were involved in publishing reliable data and avoiding medicine starvation; the second is the European Single

69 https://www.ecdc.europa.eu/en/about-uswhat-we-do/ecdcs-mission

Market which includes rules to sell drugs and medical devices or allow for health professional mobility; the third is fiscal governance. Article 168 lays down that the Union complements national policies, for instance, by supporting the "cooperation between the Member States" or adopting recommendations, while the Union respects MS health policies and organisation[70].

The European Commission coordinated a common European response to the coronavirus outbreak and took action to reinforce the EU public health sectors and mitigate the socio-economic impact across the EU. **The aim was to help MSs to coordinate their national responses and to provide objective information on the spread of the virus and effective efforts to contain it.**

The initial outbreak was coordinated at several levels, through video conferences at the European Council, through regular discussions with Health Ministers, to frequent meetings of the Health Security Committee. **Notifications regarding serious cross-border health threats were made through the Early Warning and Response System (EWRS) for communicable diseases in the EU. This system allowed EU MSs to send alerts about events with potential impact on the EU, to share information, and to coordinate their responses**. It was created by the European Commission to "ensure a rapid and effective response by the EU to events (including emergencies) related to communicable diseases". The first alert notification for Covid-19 was opened on the system on 9 January. Meanwhile the European Centre for

Tab. 2.1.1 History and trends of the initial EU response to the crisis

Source: I-Com elaboration

9 January 2020	Directorate General for Health and Safety (DG SANTE) opened an alert notification on the Early Warning and Response System (EWRS)
17 January 2020	First novel coronavirus meeting for the Health Security Committee
28 January 2020	Activation of the EU Civil Protection Mechanism for the repatriation of EU citizens
31 January 2020	First funds for research on the new coronavirus
1 February 2020	EU MSs mobilised and delivered a total of 12 tonnes of PPE to China
1-2 February 2020	447 European citizens brought home from China co-financed by the EU Civil Protection Mechanism
23 February 2020	The Commission co-financed the delivery of more than 25 tonnes of PPE to China in addition to over 30 tonnes of PPE mobilised by EU MSs and already delivered in February
28 February 2020	First procurement for medical equipment jointly with MSs

70 Art. 168 of the Treaty, points 1, 2, 6 and 7

Disease Prevention and Control (ECDC) has played a key role in assessing the threat from a scientific viewpoint. The ECDC produces rapid risk assessments, provides frequent epidemiological updates and technical support by issuing guidance on how to best face the outbreak. This guidance includes, but is not limited to, outbreak surveillance, preparedness and response planning and laboratory support.

The principal health policy action taken by the Commission was taken on 17 March 2020, after Italy had already proceeded with the introduction of its national lockdown in response to the rapid increase in cases. On that day, the European Commission set up an **advisory panel on coronavirus** made up of 7 expert epidemiologists and virologists from several MSs to formulate science-based EU response guidelines and coordinate risk management measures. The panel, which was created following a mandate by EU Member States, is chaired by the Commission President, Ursula von der Leyen, and the Commissioner for Health and Food Safety, Stella Kyriakides. **Based on the scientific advice of the ECDC, and the Covid-19 advisory panel, the European Commission published its first recommendations for community measures[71] and testing strategies[72] on 18 March**, while for Health Systems Resilience on 30 March 2020[73]. Meanwhile, the Commission decided to create a strategic RescEU stockpile of medical equipment to help EU countries during the pandemic. **The RescEU is part of the European Civil Protection Mechanism which strengthens cooperation between participating states in the field of civil protection, in order to improve prevention, preparedness and response to disasters**. The stockpile included intensive care medical equipment such as ventilators, personal protective equipment such as reusable masks, vaccines and therapeutics and laboratory supplies. The Commission financed 90% of the stockpile while the Emergency Response Coordination Centre managed the distribution of the equipment to ensure it went where it was needed most. The initial EU budget for the stockpile was €50 million. Moreover, the European Committee for Standardisation and the European Committee for Electro-technical Standardisation have established a number of European standards for certain medical devices and personal protective equipment available. This was to help both EU and third-country companies to swiftly start production and place products on the internal market more easily while ensuring a high degree of safety.

At the end of March, the pandemic was placing healthcare systems across Europe under unprecedented and increasing pressure, so the Commission issued (3 April 2020) a practical guidance for MSs to ease cross-border cooperation in transferring Covid patients for treatment in MSs where hospital beds were available, as well as medical expert teams. Regarding financial assistance for cross-border healthcare cooperation, the Commission

71 https://ec.europa.eu/info/sites/info/files/covid19_-_eu_recommendations_for_community_measures.pdf
72 https://ec.europa.eu/info/sites/info/files/covid19_-_eu_recommendations_on_testing_strategies_v2.pdf
73 https://ec.europa.eu/info/sites/info/files/background_commission_recommendations_on_health_systems_resilience.pdf

has also extended the Solidarity Fund[74] to cover public health emergencies. Thereafter, on 14 April, the Council gave its fast approval to the European Commission proposal to activate the EU's Emergency Support Instrument to directly support Member State healthcare systems in their fight against the pandemic. €2.7 billion were immediately provided, beginning where most needed, with no national envelopes. In implementing the instrument, the Commission worked in close dialogue with Member State national authorities and the European Parliament, as well as other stakeholders**.** During April, some EU countries were already studying a strategy to exit from national lockdowns through defining, tracing and testing strategies. Thus, the Commission published guidance on developing new apps that would support the fight against coronavirus in relation to data protection. The aim was to offer the framework to guarantee that citizens would have sufficient protection of their personal data and limitation of intrusiveness while using such apps. This guidance is accompanied by an EU toolbox on contact tracing apps.

Concerning Covid-19 treatment and vaccines, the EFPIA, in partnership with the European Commission, is strongly committed to the Innovative Medicines Initiative (IMI)[75]. The IMI operated until 2020 with a total budget of up to €3.276 billion. Half coming from the EU Horizon 2020 programme, and most of the rest from the EFPIA and its member companies in order to finance the largest number of projects focused on the development of therapies and diagnostics for the coronavirus SARS-CoV-2. **The selected projects are part of the common European response to the coronavirus pandemic coordinated by the Commission since the beginning of the crisis.** Furthermore, the EU, together with various partners around the world, launched on 4 May 2020 the fund-raising initiative "Coronavirus Global Response" to support "Access to COVID-19 Tools Accelerator" (ACT-Accelerator), the WHO programme established to find the resources needed to reduce the time and cost of vaccines and testing. Since then, about €16 billion have been raised (€1.4 bln directly committed by the European Commission) from donors around the world for the development of vaccines, new therapies and diagnostic tools to prevent the spread of the virus. At the same time, the Commission has mobilised around €537 million since January 2020 to develop vaccines, new treatments, diagnostic tests and medical systems to prevent the spread of the virus and save lives. These include:

- €48.2 million for 18 new research projects involving 151 teams of researchers from all over Europe and third countries;
- €100 million as a contribution to CEPI (Coalition for Epidemic Preparedness Innovations);

74 The European Union Solidarity Fund (EUSF) was set up to respond to major natural disasters and express European solidarity to disaster-stricken regions within Europe. The Fund was created as a reaction to the severe floods in Central Europe in the summer of 2002.

75 The Innovative Medicines Initiative (IMI) is a public-private partnership between the European Commission and the pharmaceutical industry, represented by the European Federation of Pharmaceutical Industries and Associations (EFPIA), to improve health by accelerating the development of innovative medicines and patient access to them, especially in areas where there is an unmet medical or social need.

- €25.25 million for the Europe-Developing Countries Clinical Trials Partnership;
- €72 million (compared to 45 million initially planned) from the HORIZON 2020 programme to the Innovative Medicines Initiative;
- €6 million mobilised by the Health Knowledge and Innovation Community of the European Institute of Innovation and Technology;
- €156.63 million for innovative solutions to face the coronavirus emergency, of which a 150 million additional contribution entirely dedicated to fighting the pandemic;
- €129.45 million to strengthen production and deployment capacity and improve the understanding of the pandemic.

In addition, the Commission offered CureVac, a highly innovative European vaccine development company, financial support through a €75 million loan guarantee from the European Investment Bank (EIB). The EIB also signed a €100 million financing agreement with the immunotherapy company BioNTech SE for the development of a vaccine programme. EIB financing was supported by both the HORIZON 2020 programme and the Investment Plan for Europe. **On 28 May 2020, the Commission announced the next steps of the "Coronavirus Global Response" initiative in favour of universal access to affordable treatment and vaccines**. Together with the international organisation Global Citizen, the launch of the awareness-raising campaign "Global Goal: Unite For Our Future" was planned, to mobilise additional funding to develop and distribute vaccines, tests and treatments against the coronavirus, ending on 27 June 2020 at the World Donor Summit. EFPIA also supported the European Commission together with Vaccines Europe, to ensure that vaccines developed against Covid-19 would have been accessible to citizens throughout Europe, as quickly as possible, as set out in the EU Vaccines Strategy Covid-19, published on 17 June 2020[76].

The strategy, which is part of the set of initiatives developed by the EU to address the health emergency and provide concrete responses to the needs of the population, aims to achieve three main objectives:

1. ensure the quality, safety and efficacy of vaccines, supporting research at European level in compliance with the regulatory framework;
2. ensure timely access to vaccines for all MSs and their citizens, while continuing efforts at the level of international cooperation and solidarity;
3. ensuring fair access within the single market, especially for prices.

More recently, on 19 January 2021, the European Commission adopted a **Communication calling on Member States to speed up the rollout of vaccines** across the EU. By mid-July, Europe had enough vaccine doses to vaccinate 70% of the EU adult population. Moreover, in order **to ramp up industrial vaccine production in the EU** on 4 February 2021, the European Commission set up a **Task Force**, under the authority of the Commissioner for the Internal Market and in

76 European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL AND THE EUROPEAN INVESTMENT BANK – EU Strategy for COVID-19 vaccines

cooperation with the Commissioner for Health and Food Safety, in order to increase production capacity for vaccines in the EU and act as a one-stop-shop for manufacturers in need of support, addressing bottlenecks in production and supply chains. The regular contacts of the Task Force with industry and MSs allow the Commission to have **a good understanding of vaccine production capacities in the EU**. This is the case today with the EU sharing the information through a constantly updated interactive map[77].

At the same time, the EU realised that old approaches to health and pharmaceutical policies had not worked well**, thus, the Commission launched a public consultation to evaluate a strategy to ensure affordability, sustainability and security of supply for innovative drugs and beyond**. The pandemic has shown that the **EU needs a crisis-resilient system and the means to produce medicines within the EU to ensure timely access to essential medicines for citizens and hospitals in all situations**. The initiative was launched on 2 June 2020, and until 7 July all stakeholders had been able to send feedback. Following this first phase, the various provisions were officially published on the basis of the feedback received during the public consultation open from 16 June to 15 September 2020. **The entire package was adopted on 25 November 2020**[78] with the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "A pharmaceutical strategy for Europe". The EU thus launched a new strategy to improve and accelerate patient access to safe and affordable medicines and to support innovation in the EU pharmaceutical industry[79]. **Then, as part of the EU pharmaceuticals strategy, and drawing lessons from the pandemic**, the Commission has begun to plan the **evaluation and revision of the EU's general legislation on medicines** for human use to ensure a future-proof and **crisis-resistant medicines regulatory system** whose final adoption is **foreseen for the end of 2022**.

2.1.3. Institutional lessons learned after the first phase of the pandemic

Since the beginning of the pandemic, European countries have put into place heterogeneous responses. How each country has responded to the emergency not only reflects the objective needs of that country (number of fatalities, share of older people or people infected, etc.), but, instead, the differences in the features of its national system and, almost without exception, the country's self-interests. **A key political lesson of this crisis is that further collaboration is required in Europe to face health challenges such as the Covid-19 pandemic. And the European Union seems to have understood the lesson.** One way to

77 https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/public-health/eu-vaccines-strategy_en

78 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12421-Pharmaceuticals-safe-and-affordable-medicines-new-EU-strategy-_en

79 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12421-Pharmaceuticals-safe-and-affordable-medicines-new-EU-strategy-_en

overcome problems of collective action seemed to be to create a public health authority at the European level, with powers beyond the limited coordination activities carried out by the ECDC. The management of pandemics does not respect borders and requires forms of collective action to face the challenges. **The EU, not being a "federal" entity, needs to adopt some institutional frameworks to enforce cross-country collaboration to this end**. The President of the European Commission, Ursula von der Leyen, in her first speech on the State of the Union, at the Eurocamera, in Brussels (16 September 2020) first announced that with the Italian Presidency of the G20, the Commission would organise a Global Health Summit in Italy to show that Europe is there to protect its citizens. The aim is to build a Health Union, said von der Leyen, as the pandemic is not at its end and recovery is still in its early stages. For this reason, the EU must act with responsibility and unity. Von der Leyen announced the establishment of a new European Agency following an idea emerging from the Macron-Merkel summit on 18 May 2020, where it was clearly stated that Europe should regain sovereignty. It was then taken up in the conclusions of the European Council of 17-21 July. The Agency traces, with the appropriate differences, the USA BARDA (Biomedical Advanced Research and Development Agency) model. **The European Health Emergency Preparedness and Response Authority (HERA) was established on 16 September 2021.** The HERA will support the preparation and response capacity for trans-national health emergencies, both of natural and artificial origin and should be part of the European health self-sufficiency programme, especially in the field of pharmaceutical sector dependence on global supply chains. The establishment of a European Biomedical Advanced Research Agency allows not only for overcoming the fragmentation of the expertise currently scattered among various European bodies and organisations, but also plays the role of coordinating the research of diagnostic and therapeutic solutions so as to be prepared for the management of epidemic and pandemic emergencies, which are, unfortunately, expected to reoccur. In short, the creation of such an agency involves the strengthening of the role of the ECDC whose mandate is to work with national and EU-level health authorities to facilitate cooperation, and to provide the evidence base needed for effective action.

2.2. TOWARDS A EUROPEAN HEALTH UNION

The Covid-19 has spread across Europe, and disproportionately hit older and more fragile people, showing a clear social gradient in correlated deaths. Countries that had been better prepared and acted quickly to reduce the spread of the virus through the rapid scaling-up of testing, tracking and tracing strategies, were more able to avoid the more stringent and costly containment and mitigation measures. Meanwhile, policies to temporarily increase hospital beds and equipment have helped deal with the surges in demand, however, the most significant, though indirect, help was provided by reinforcing local healthcare, particularly home assistance.

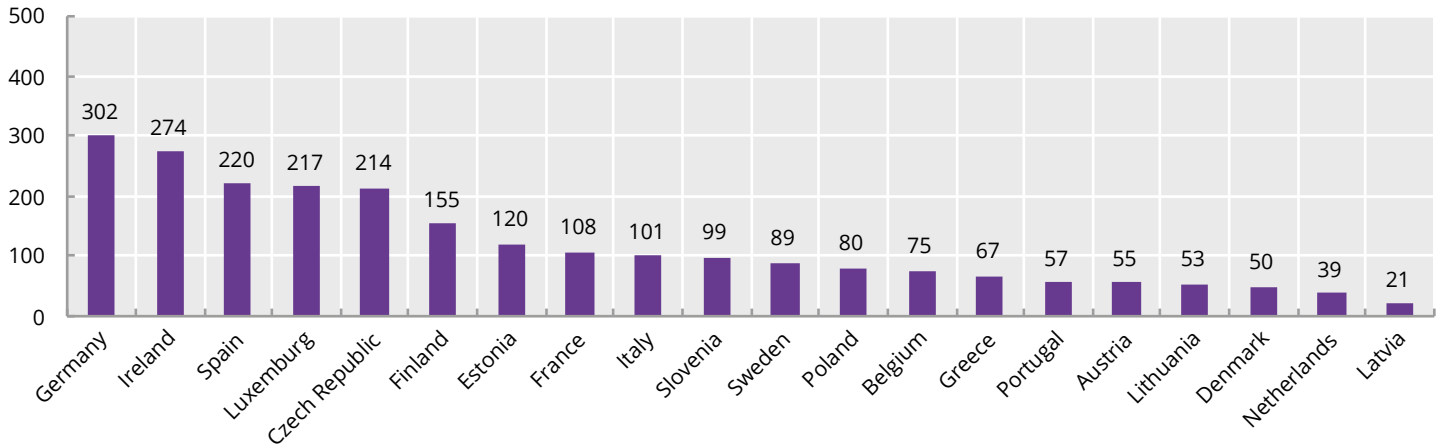
Furthermore, many non Covid-19 patients were unable to access needed care during the first peak of the pandemic in spring 2020, and the reductions in prevention and control also followed into the next months. People with emergency health needs have sometimes struggled to receive timely acute care, and those with chronic health conditions have faced disruptions to their routine treatment. The pandemic has, therefore, put an immense strain on European countries, testing the resilience of every country's health and economic systems, together with the ability of the European Commission to develop a coordinated set of responses to what is still a common threat.

Generally speaking, the pandemic showed that a lack of investment in health systems, while saving money in the short term, can have devastating effects on the economy and society in the long term. Moreover, it has highlighted that other health emergencies will occur in the future, especially concerning the increasing burden of non-communicable diseases which will require placing the patient at the centre of health policies and the uptake of new innovations in treatment. Consequently, health expenditure should be regarded as an investment for our societies, rather than a cost, avoiding health budgets being cut as a consequence of economic recession. The central governments of the European Member States increased their health spending in response to the health emergency during 2020 (Fig.2.2.1). As well, the **EU launched the extraordinary Next Generation EU (NGEU) programme**. It is a special fund aimed at financing economic recovery in the coming years, with the issuance of European bonds that **will serve to support projects and structural reforms established by the Recovery Plan (reforms and investment) in each of the 27 EU Member States**. In total, the forecasted sum is **€750 billion**, made up of €390 billion in grants and €360 billion in loans, divided according to the different needs of the Member States most affected by Covid-19.

According to the OECD (2020), **the pandemic introduced a new concept of resilience**, acknowledging that massive disruptions can and will happen, and it is essential that core systems must be able to **recover and adapt**. This new approach to resilience should focus on "the ability of a system to **anticipate, absorb, recover from, and adapt** to a wide array of systemic threats."

Fig. 2.2.1 Central government additional Covid-19 health spending commitments per capita (EUR PPP, 2020)

Source: OECD member country governments



The EU's institutional response has been mainly (though not exclusively) led by the European Commission, and through European Council member meetings. The European Parliament and European Central Bank have also played important roles.

The EU public health response has mainly involved:

- Direct financial support for procurement programmes to support healthcare systems;
- Support for research in treatments and vaccines;
- Medical guidance for Member States;
- Coordinating the supply and manufacturing of Personal Protective Equipment (PPE).

A number of collaborative EU-level initiatives have helped alleviate supply constraints and support a more coordinated response across countries. Notable actions include:

- **Joint procurement.** The European Commission has launched several voluntary Joint Procurement procedures since February 2020. These are based on Article 5 of Decision 1082/2013 on cross-border health threats[80], as well as on the Joint Procurement Agreement (JPA) with participation open to all EU and EEA Member States;
- **Seven international tenders** launched to address or prevent shortages of medical countermeasures relevant for Covid-19. The European Commission helped countries identify and select suppliers, and negotiate contracts, enabling them to purchase

80 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D1082&from=EN

essential products under the same conditions;

- **Clearing house**[81]. The European Commission set up a temporary clearing house to facilitate matching supply and demand between manufacturers and MSs, operatig from 1st April 2020 for a period of six months. It used a centralised platform that pools data on trade flows, production capacity in third countries, together with logistical, technical and regulatory bottlenecks;
- **Enhanced monitoring**. The European Medicines Agency, together with the pharmaceutical industry and EU MSs, launched a fast-track monitoring system to help anticipate drug shortages. This reinforced a single contact point for national medicine agencies (SPOC) and the launch of an industry single point of contact (i-SPOC);
- **Strategic stockpiling**. The EU reinforced and strengthened components of its disaster risk management by upgrading the EU Civil Protection Mechanism[82]. The latest element introduced is RescEU, established in March 2020 as a common reserve of medical equipment managed autonomously by the European Commission;
- **Manufacturing capacity**. Although Europe has a strong manufacturing footprint, the supply chain still relies heavily on subcontractors to produce pharmaceutical raw materials outside the EU borders. The European Commission's new pharmaceutical strategy[83] emphasises policies to increase the manufacturing capacity for certain critical medicines, active pharmaceutical ingredients and raw materials within Europe;
- **Trade policies**: regulating exports and liberalising imports. A temporary EU-wide export authorisation scheme for personal protection equipment (PPE) set out conditions for their export during the very first wave of the epidemic. In April 2020, customs duties and VAT were waived on imported medical devices and PPE from non-EU origins. Moreover, the EMA published guidance on regulatory expectations and flexibility during Covid-19, where MSs may "grant full or partial exemption to certain labelling and packaging requirements" for crucial medicines used for Covid-19[84];
- **Vaccines**. The EU Vaccine Strategy[85] outlined how the European Commission intended to accelerate the development and availability of Covid-19 vaccines. Its main objectives are to secure the production of vaccines within the EU; to ensure their availability for its MSs through Advance Purchase Agreements with vaccine producers; and to adapt EU rules to accelerate the development, authorisation and availability of vaccines while maintaining safety standards.

However, the EU struggled to play a coordinating role, complementing national policies to help

81 https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/emergency-support-instrument/covid-19-clearing-house-medical-equipment_en
82 https://ec.europa.eu/echo/what/civil-protection/mechanism_en
83 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2173
84 Article 63(3) of Directive 2001/83/EC
85 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1103

countries in facing common challenges, such as a lack of sufficient healthcare organisation and provision, so that each Member State was better prepared for the healthcare challenges posed by the virus. Since the beginning European countries have adopted different responses to the same pandemic. Indeed, while most federal states have an authority or an agency with such a remit, and responsibilities on global health and epidemic intelligence, the equivalent did not exist for the EU at that time. In the latter, responsibilities are decentralised to MSs, which only began sharing information after the **European Centre for Disease Prevention and Control (ECDC)** was established in 2005[86], with limited functions and not being involved in public health decision making. **During the pandemic, we witnessed European MSs confusing information, communications and decisions about the vaccination campaign** concerning the monitoring of the safety of one of the Covid-19 vaccines. **All of this has created great damage in terms of public confidence, and curbed the vaccination campaign**. The EMA participation was messy, and information leaks did not help. Thus, **the key political lesson from this crisis is that further collaboration is required in Europe to face health challenges** and, fortunately, the EU seems to have learnt the lesson, even if **many foreseen and proposed actions still need to be established.**

"*We cannot wait for the end of the pandemic to repair and prepare for the future. We will build the foundations of a stronger European Health Union in which 27 countries work together to detect, prepare and respond collectively*". So declared Ursula von der Leyen, President of the European Commission, speaking at the World Health Summit (25 October 2020). **Therefore, the European Commission is committed to building a strong European Health Union**, where all EU countries prepare and respond together to health crises, with available, affordable and innovative medical supplies, and where countries work together to improve prevention, treatment and aftercare for diseases such as cancer. The European Health Union should better protect the health of its citizens, equip the EU and its MSs to better prevent and address future pandemics and improve the resilience of Europe's health systems. **The key initiatives** to build a European Health Union include **a Pharmaceutical Strategy for Europe, crisis preparedness and response measures and the European Plan to Beat Cancer**.

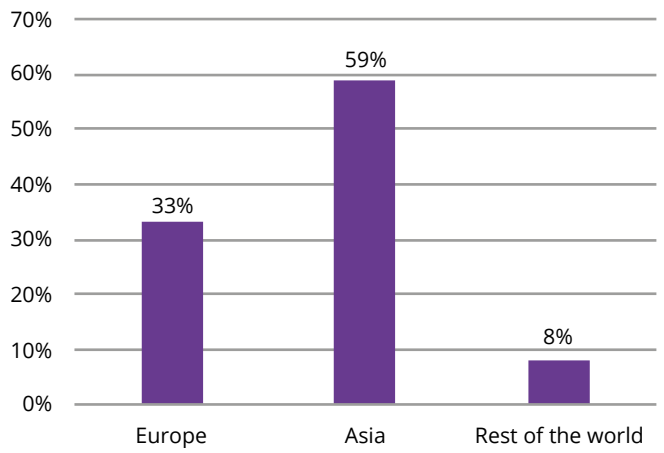
2.2.1. The Pharmaceutical Strategy

The pandemic caused by the SARS-CoV-2 virus clearly demonstrated the need to **revise how the Union supplies medicines to its population**, as well as highlighting the importance of establishing the conditions and means to produce medicines within the EU, **guaranteeing accessibility, sustainability and safety**. Returning the **production of pharmaceutical raw materials to Europe is one of the cornerstones of this strategy**, as is the need to increase innovation in the areas of unmet needs. Indeed, although Europe has a strong manufacturing footprint, the **supply chain**

86 https://www.ecdc.europa.eu/en/about-uswhat-we-do/ecdcs-mission

Fig. 2.2.2 Geographical allocation of active principles producers (% value, 2020)

Source: Certificate Database, European Directorate for the Quality of Medicine & Healthcare



still relies heavily on subcontractors to produce pharmaceutical raw materials outside the EU. The result is that between 60% and 80% of the active chemical ingredients are produced outside Europe, mainly in China and India.

Other factors connected with the emergency have also contributed to the shortage of medicines in Europe, jeopardising the management of the health emergency. First of all, there was the sudden increase in demand for some medicines, especially in intensive care units. In addition, the population reacted to the pandemic by cramming stocks of non-prescription pain relievers. Consequently, the growing demand for all these medicines threatened their availability for patients who take them regularly to control chronic and/or rare diseases.

At the same time, the supply side suffered from export bans together with the building up of stocks of medicines at national level, the reduction in production capacity, and the closure of suppliers of raw materials/active pharmaceutical substances. Logistical problems and difficulties in cross-border transport further affected the availability of drugs, as well as the development of new therapies against Covid-19.

On 1st June 2020, the European Commission began working on this problem, publishing a roadmap for drawing up a European Pharmaceutical Strategy and launching a public consultation. The aim was to promote competitiveness, the ability to innovate and the sustainability of the EU pharmaceutical industry. On **25 November 2020, the Commission published the final document of the Pharmaceutical Strategy for Europe**[87], in line with the new Industrial Strategy for Europe and the priorities outlined in the European Green Deal, with the European Cancer Plan and the European Digital Strategy. Since the publication of the strategy roadmap in June 2020, the Commission has conducted a series of consultations and meetings to inform the designing of the strategy and additional consultation activities are planned in the implementation phase. In particular the combined evaluation roadmap/inception impact assessment has been opened to consultation since 30 March to 27 April 2021[88] and, thus, the latest public consultation was opened on **28 September**

87 https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020DC0761&from=EN

88 file:///C:/Users/User/Downloads/090166e5db8a9d7c.pdf

2021 and will close on 21 December 2021[89]. **It builds further on the public consultation conducted for the preparation of the Pharmaceutical Strategy** for Europe of November 2020 and it aims to collect views of stakeholders and the general public in order to support the evaluation of the existing general pharmaceutical legislation on medicines for human use, and the impact assessment of its revision to ensure a future-proof and crisis-resistant medicines regulatory system.

Specifically, the strategy is divided into four objectives as below.

The main initiatives of the strategy include:

- **The revision of basic pharmaceutical legislation** to be adapted to future needs and encourage innovation;

Tab. 2.2.1 A Pharmaceutical Strategy for Europe

Source: European Commission

Objectives	Description
1	Provide patients with access to affordable medicines and address unmet medical needs.
2	Promote the competitiveness, innovation capacity and sustainability of the EU pharmaceutical industry and the production of high quality, safe, effec-tive and greener medicines.
3	Strengthen emergency preparedness and response mechanisms and ad-dress the issue of security of supply.
4	Ensure a solid position of the EU on the world stage by promoting high standards in terms of quality, efficacy and safety.

- **The creation of an EU authority for preparedness and response** to health emergencies;
- The **revision of the regulations on medicinal products** for paediatric use and rare diseases;
- The **launch of an open and constructive dialogue between all those involved in pharmaceutical production and public authorities**, to identify the fragility of the global supply chain and define strategic options to strengthen the continuity and safety of the supply in the EU;
- **Collaboration between national authorities on pricing, payment and procurement policies** to increase the sustainability of health systems;
- The creation of a **robust digital infrastructure**, including a proposal for a European health data space;
- **Support for research and innovation**, mainly through Horizon 2020 and EU4Health;
- **Actions to promote innovative approaches to European research and development and public procurement**, regarding antimicrobials and their alternatives, and measures to restrict and optimise their use.

The new European authority, HERA (Health Emergency Response Authority), established on 16th September 2021[90] **and built** on the model of BARDA, the US authority for research and development in the biomedical field, **is intended also to be a reference point for programming,** knowing and evaluating the

89 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12963-Revision-of-the-EU-general-pharmaceuticals-legislation/public-consultation_en

90 see paragraph 2.1.3 and https://ec.europa.eu/health/sites/default/files/preparedness_response/docs/hera_2021_comm_en.pdf

upcoming innovation in order to reap the benefits of innovation and deploy tools to support market access. HERA will indeed **anticipate threats and potential health crises**, through intelligence gathering and building the necessary response capacities. Not only when an emergency hits, HERA will ensure the **development, production and distribution of medicines, vaccines and other medical countermeasures** but it will work on **preparedness** before a potential emergency spreads. It means that HERA will work closely with other EU and national health agencies, industry and international partners to improve the EU's readiness for health emergencies. The authority will carry out **threat assessments and intelligence gathering**, develop **models to forecast an outbreak** and by early 2022 and it will **support research and innovation** for the development for new medical countermeasures, including through Union-wide **clinical trial networks and platforms for the rapid sharing of data**. Last but not least HERA will address market challenges and work to **boost industrial capacity**. With this last objective the authority will establish a close dialogue with industry, a long-term strategy for manufacturing capacity and targeted investment, and address supply chain bottlenecks for medical countermeasures.

Bringing the production of pharmaceutical raw materials back to Europe is the cornerstone of this strategy, requiring the design of **an adequate industrial policy, and the creation and preservation of incentives. The latter obviously also depends on, but not only, the definition of the price negotiation by MSs**. An interesting example is France, which is preparing a pricing strategy for pharmaceuticals, that guarantees a higher price when they come entirely from French territory. Negotiations usually do not consider this aspect, and the evaluation often focuses only on economic convenience. **In general, some risks may be related to some of the proposals contained in the strategy**, depending on how the proposals will be implemented through actions. These are partly related to the multi-year duration of the review process, and partly to the possible erosion of patent rights. The strategy specifically planned an impact assessment for some changes to the European regulations concerning medicines for rare diseases (Regulation No. 141/2000) and paediatric medicines (Regulation No. 1901/2006), and to investigate the effectiveness of the incentives introduced by the two regulations. Both[91] support research and development and, according to the scientific literature, have brought clinical benefits. Furthermore, many small-medium companies have approached the orphan drug market, albeit still immature, using the relevant regulatory paths. Consequently, a **fear is that a revision of the legislation could undermine the level of innovation in disease treatments, without actually creating added value in terms of access**. Here, it **is worth mentioning that patient access to medicines still varies greatly amongst MSs** (Fig. 2.2.3), and that the commitment to reducing these differences could result in both **equity**

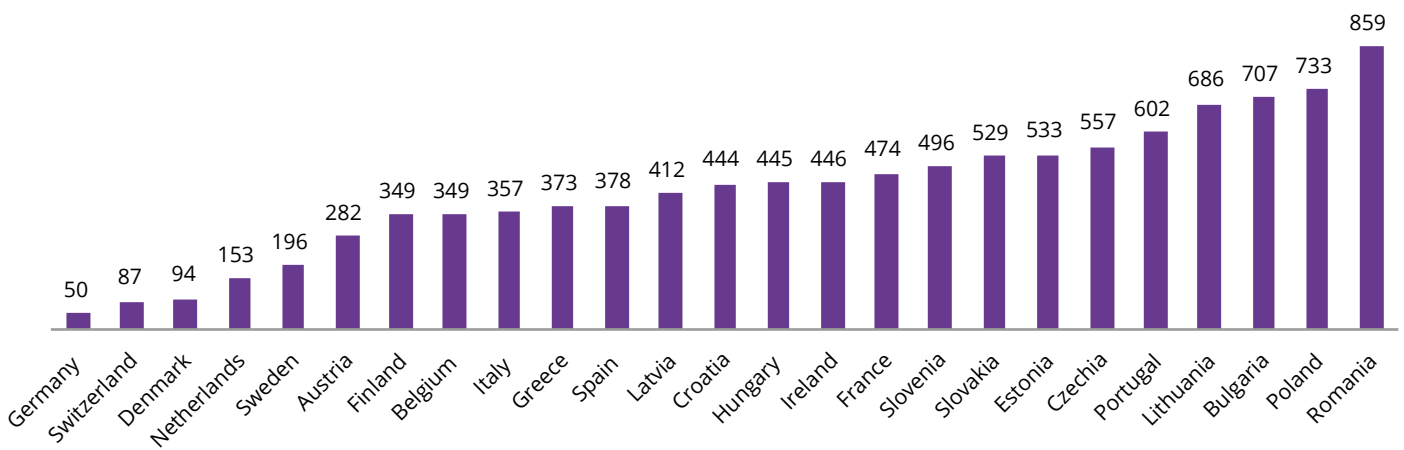
91 Oriol Solà-Morales, Journal of Market Access & Health Policy, "Has OMP legislation been successful? Yes, though the orphan drug market remains immature" (2019)

in access for citizens and the willingness to innovate for firms. The public consultation followed the Inception impact assessment on both regulations and lasted from 7th May 2021 to 30th July 2021. The Commission adoption is planned for the first quarter of 2022[92].

The baseline for the strategy was of course **the immediate urgency for Europe** to ensure the **speed up in** Covid-19 **vaccines production and the respect of agreements** to guarantee the expected deliveries. The short – term objective was to have these medicines developed in Europe also with a view to future production capacity. **The medium – long term objective is instead to overcome the fragmentation of the health ecosystem also by an industrial point of view**. The main challenges to be addressed are the **supply chain vulnerabilities, health care capacities constraints, and fragmentation**. As far as the supply chain is concerned the EU need to consider also skill shortages, and pay and working condition which prevent the skilled staff from staying in the long run. Moreover**, public buyers are still awarding contracts mainly basing on the best bidder** (lowest price) and this contributes **to reducing the number of suppliers in the EU**. Thus, while working on the industrial side the EU also need to

Fig. 2.2.3 Median time to availability for all new medicines (days, 2015 - 2019)

Source: EFPIA



92 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12767-Medicines-for-children-&-rare-diseases-updated-rules_en

work in order to **increase capacity building, and the digital upskilling of employers working in the health sector while intervening to leverage the health data potential**, which is still underdeveloped and underused. That is why one of the corollary initiatives of the pharmaceutical strategy are the European Health data space and Eu4health and, of course **it is a matter of time**. The ambition is to **have a reform for the pharma strategy packet by the end of 2022**.

2.2.2. Crisis preparedness and response measures

Early lessons learnt from the pandemic have shown **that the current system has not been able to ensure an optimal response at EU level**. The current health security arrangements, established by Decision No 1082/2013/EU on serious cross-border threats to health[93], provide a limited legal framework for EU level coordination, based essentially on the Early Warning and Response System (EWRS) and the exchange of information and cooperation within the Health Security Committee.

Due to **unpreparedness combined with the gradual time-spatial transmission** of the virus, Phase 1 of the epidemic in the EU was initially characterised by regulatory variations (Fig. 2.2.4) across MSs, but then was promptly replaced by a **spontaneous regulatory convergence**. It is worth noting that this convergence among EU MSs' national responses occurred spontaneously, **with no direct role played by the EU and its cross-border health emergency coordination mechanisms**.

93 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D1082&from=EN

The key lessons learned during the health emergency, include the **need to increase and improve capacities for surveillance, preparedness, early warning, risk assessment and response as well as the operation of the key EU structures and mechanisms** thus reinforcing both the health response of the EU agencies, and international cooperation. Answering to the lesson learned requires to **a stronger and more comprehensive health security framework** for the Union, in order to prepare and respond to health crises.

The question is: how these instruments can be prepared to work?

The EU proposal thus includes the extension of the mandate of the ECDC to support the Commission and Member States in the following areas:

- Prevention of communicable diseases and specific health issues, e.g., antimicrobial resistance, vaccination and biosecurity;
- Preparedness and response planning;
- Reporting and auditing epidemiological surveillance via integrated, digital systems enabling real-time surveillance;
- Provision of non-binding recommendations for risk management;
- Coordination of new networks including EU reference laboratories.

At the same time the EU understood that industries need to partner up with institutions for better collaboration, and to **avoid shortages and increase capacities of production**. That is the reason why EMA is the second EU agency whose role and operation need to be reinforced.

The Parliament and the Council have come to an **agreement on 28th October 2021** to **strengthen the EMA's role** to avoid potential future shortages of medicines and medicines devices. In order to do so, two new mechanisms were agreed upon. First, two "shortage steering groups" will be created, one for medicines and one for medical devices. Both of these groups will work closely with representatives of health care professionals, representatives of patients, but also with marketing authorisation holders and wholesale distributors. These steering groups will meet on a regular basis and when the situation requires, before or during a public health emergency. A European shortages monitoring platform will also be created to easily collect information on shortages, supply and demand of medicines, including a public web page to allow citizens access to potential ongoing shortages. "With the new European Shortages Monitoring Platform, we provide the Agency with a key tool to monitor medicines supply and prevent shortages", said the rapporteur Nicolás González Casares (S&D)[94]. In this context it is crucial to have monitoring and reporting procedures, and to develop IT tools to check on supplies chain in order to prevent major crisis from escalating. Moreover. it is essential to be aware of which medicines are more critical and monitor their supply and demand through the close collaboration between member states and industry. Moreover, the EU will establish an Emergency Task Force that will be built as a membership to include various Agency committees and working groups, the Co-ordination Group for Mutual Recognition and Decentralised Procedures (CMD(h)), and the Clinical Trials, Coordination and Advisory Group (CTAG)).

The European Commission proceeded with a **Proposal for a Regulation on Serious Cross-border Health Threats** repealing Decision 1082/2013/EU[95], in order to create a more robust mandate for coordination at EU-level. Parliament's Committee on the Environment, Public Health and Food Safety adopted the report in committee on 13 July 2021. The Council agreed its position on 23rd July 2021. **The Parliament voted the committee report in plenary on 15th September 2021**, thereby setting its negotiating mandate and opening the way for interinstitutional negotiations.

The Proposal for a Regulation on Serious Cross-border Health Threats:

- Sets out a **comprehensive legislative framework to govern action at Union level** on preparedness, surveillance, risk assessment, and early warning and responses;
- Enhances the Union's **guidance in the adoption of common measures at EU level** to face a future cross-border health threat.

The regulation applies to threats of biological origin (communicable diseases, antimicrobial resistance and biotoxins), threats of chemical origin, threats of environmental and unknown origin, and events which may constitute public health emergencies of international concern under the International Health

94 https://www.europarl.europa.eu/news/en/press-room/20211019IPR15235/deal-on-stronger-role-for-eu-medicines-regulator

95 https://ec.europa.eu/info/sites/info/files/proposal-regulation-cross-border-threats-health_en.pdf

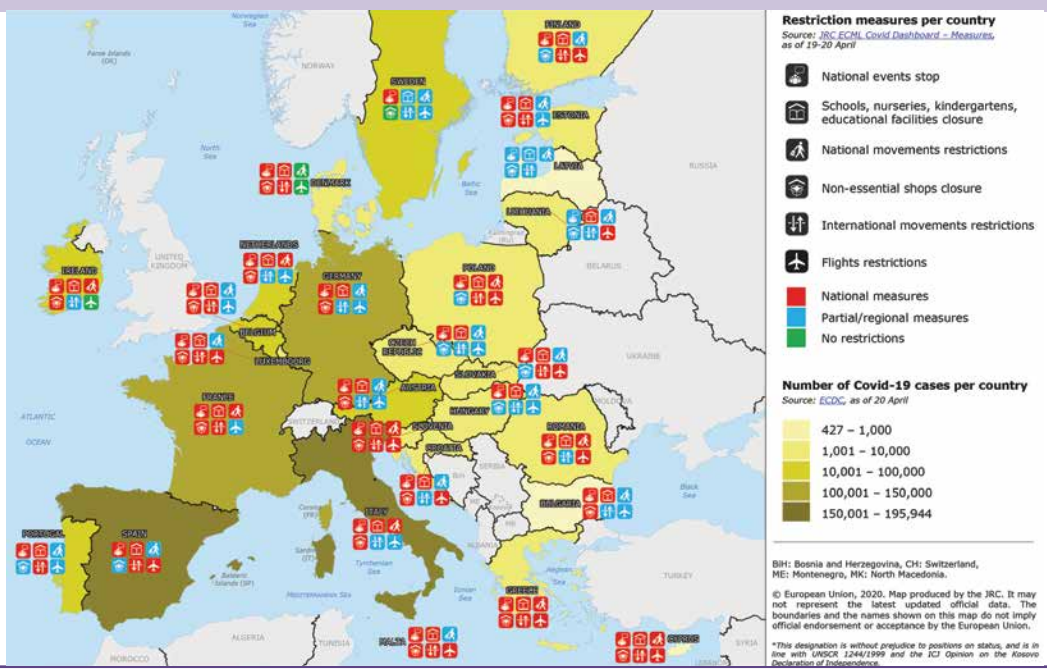
Regulations (IHR), provided that they fall under one of the previously listed categories.

The main operative consequences would be the creation of an EU health crisis and pandemic preparedness plan, complemented by national plans and transparent reporting of capacities, strengthened and integrated surveillance systems, enhanced risk assessment for health threats, increased power to enforce a coordinated response at EU level through the Health Security Committee, and an improved mechanism for recognition of and response to public health emergencies. **Moreover, it provides for the strengthening of the EU's key public health agencies –** the European Centre for Disease Prevention and Control (ECDC) and the European Medicines Agency (EMA).

The European Commission and the ECDC will regularly test and audit pandemic preparedness plans at EU and national levels, and **report results to the MSs and European Parliament**, while MSs will be required to improve their reporting of health system indicators. **What is still not clear, is the possible effect on MSs of the preparedness evaluation conducted by the agency**. However, the proposal is accompanied by two further proposals to extend the mandate of the EMA

Fig. 2.2.4 Covid-19 restriction measures in the EU during Phase 1 (April 2020)

Source: JRC



and of the ECDC[96]. The **package of three proposals** was discussed during the **conference of the Council of the European Union in June 2021** in which the Council agreed its position. Parliament's plenary adopted the report on 8th July 2021, while the interinstitutional trilogue negotiations started on 13th July 2021.

2.2.3. Europe's Beating Cancer Plan

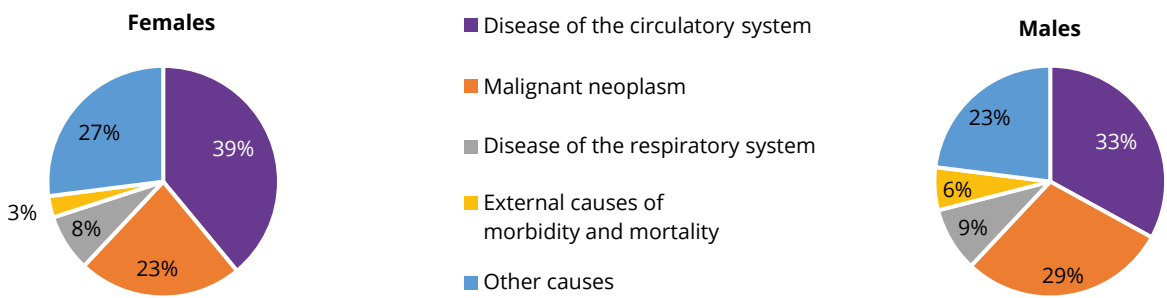
Since **cancer is the second leading cause of mortality in EU countries after cardiovascular diseases**, accounting for 29% of all deaths among males and 23% among females across all EU Member States, improving prevention and care is vital. 40% of cancer cases in the EU could be prevented but only 3% of health budgets are spent on health promotion and disease prevention[97].

Moreover, a **number of non-communicable diseases share common risk factors and their prevention and control** would benefit most citizens.

The disease burden of cancer (total number of Disability-Adjusted Life Years) has increased and **malignant neoplasms cause the second-greatest share of DALYs, increasing from 19% to 20%** of the total in the last fifteen years. Cancer could soon surpass cardiovascular diseases as the disease group causing the greatest societal burden, having already done so in many wealthy countries. Moreover, we expect that Covid-19 will create in the very near future a "cancer epidemic" due to the worsening in screening, monitoring and following therapy among target population groups and cancer patients. The IARC (International Agency for Research on Cancer) estimates there will be a substantial growth in

Fig. 2.2.5 Main causes of mortality among women and men in the EU

Source: Eurostat

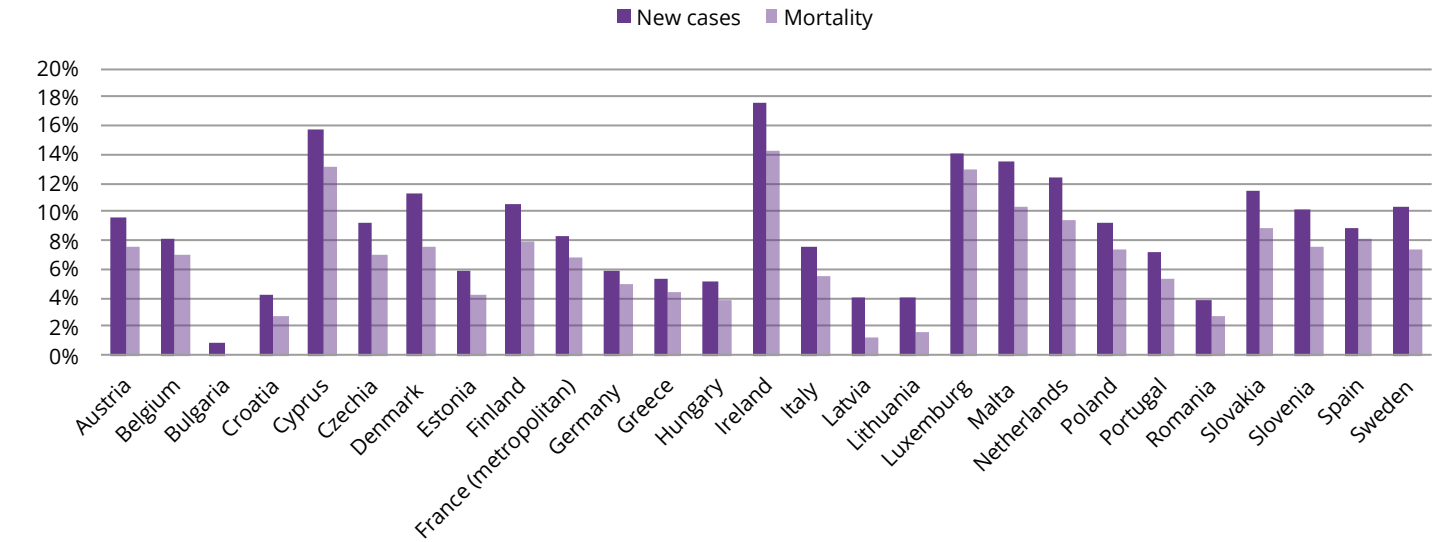


96 https://ec.europa.eu/info/sites/info/files/proposal-mandate-european-medicines-agency_en.pdf
https://ec.europa.eu/info/sites/info/files/proposal-mandate-european-centre-disease-prevention-control_en.pdf

97 Europe's Beating Cancer plan – Let's strive for more.

Fig. 2.2.6 Predictions for all cancers, new cases and mortality change per country (2025 vs 2020, Δ %)

Source: IARC



new cases and mortality among European countries in the next five years (Fig. 2.2.6).

Europe's Beating Cancer Plan was launched on World Cancer Day on 4th February 2020, in an event in the European Parliament in Brussels, supported by the MEPs Against Cancer Interest Group. The mission letter to the Health Commissioner Stella Kyriakides defined **the four pillars of Europe's Beating Cancer Plan – prevention, early diagnosis, treatment and follow-up care**. The plan is linked to other priorities of the new Commission and has the support of the MEPs, Member States and stakeholders who work together with the Commission to improve cancer prevention and care in Europe. Speaking in the European Parliament, the Commissioner gave an indication of what the plan could focus on, specifying a horizontal approach addressing key determinants, such as tobacco consumption, alcohol abuse, physical exercise and healthy diets, as part of a prevention-focused strategy. On 4th February 2020, the European Commission opened a public consultation on the plan (that lasted 12 weeks until 21st May 2020) inviting all interested individuals or organisations to share their views and experiences to feed into a European cancer plan putting European citizens at the centre. **The plan was then adopted on 3rd February 2021**[98]. **The actions**

98 Communication From The Commission To The European Parliament And The Council. Europe's Beating Cancer Plan. Brussels 3/2/2021.

and flagship initiatives[99], finally included in the plan, cover and tackle the entire pathway of the disease – prevention, diagnosis, treatment and quality of patients and survivors. Europe's Beating Cancer Plan is a political commitment to turn the tide against cancer and another stepping stone towards a strong European Health Union. Europe's Beating Cancer Plan will focus on research and innovation, tap into the potential that digitalisation and new technologies offer, and mobilise financial tools to support MSs. With its policy objectives, supported by ten flagship initiatives and multiple supporting actions, the Cancer Plan will help MSs turn the tide against cancer. It will enable expertise and resources to be shared across the EU supporting countries, regions and cities with less knowledge and capabilities. It will help researchers to exchange findings in the EU and access crucial health data on the potential causes of cancer and its promising treatments. Medical staff and hospitals will be able to tap into a wealth of shared information. Ultimately, it will ensure that patients across the EU can benefit from better care and treatment.

Making the most of data and digitalisation in cancer prevention and care is one of the key issues of the plan, and the Commission underlines that the digital transformation can bring significant benefits for the health sector. As much as 30% of the world's stored data is currently produced by health systems, but **the health sector lags behind in exploiting this potential and making information out of data.** Cancer care is one of the major disease areas that will benefit from the European Digital Strategy, the Commission says, thanks to better exploitation of real-world data and using powerful tools such as Artificial Intelligence and high-performance computing. **The European Health Data Space (EHDS) will enable cancer patients to securely access and share their health data in an integrated format** in the electronic health records between healthcare providers and across borders in the EU. The Commission will pursue work with Member States on a common exchange format for electronic health records and to tackle data security, privacy and interoperability. **The Commission will establish the EU Cancer Plan Implementation Group**, to align actions and policies across the European Commission and other EU institutions. **It will work closely with the European Parliament committees** that deal with cancer-related issues; Member States (through the Steering Group on Health Promotion, Disease Prevention and the Management of Non-Communicable Diseases); the Cancer Mission Board functioning as a scientific advisory group; and a stakeholder contact group, mainly involving patient groups, established under the Commission's Health Policy Platform. The Commission will meet with representatives of these institutions and stakeholder groups at regular intervals, at least twice per year, and the Cancer Plan will be monitored through **an implementation roadmap and progress indicators**.

99 https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-health-union/cancer-plan-europe_en#flagship-initiatives

2.3. THE EU HEALTH DATA SPACE AND ITS CRUCIAL ROLE FOR A STRONGER EU HEALTH UNION

The emergence of new technologies and **enhanced connectivity** have spurred the **exponential growth of health data**. However, a vast quantity of this remains hidden in private or proprietary and project specific registries. Nevertheless, the promotion of health-data exchange is highly important in **supporting clinical research, guaranteeing new treatments**, medicines, medical devices and health outcomes and to enhance the responsiveness of the whole system.

Both electronic **health records and personally-generated health data**, for example, from wearable devices, smart sensors and health apps provide **valuable information** on health outcomes and **bring deeper insights** into lifestyle patterns and environmental risks that contribute to the prevalence of chronic and/or non-communicable diseases.

Being able to use this information extensively opens up new possibilities in the field of healthcare, especially in **personalised healthcare and precision medicine**.

However, there are challenges such as limitations and obstacles created by interoperability and the differing legal regimes within the EU that govern the access and right to process health data for research purposes, a lack of high quality data, organisational and structural barriers and the need for a highly ethical approach essential to build trust with individuals and strives to use the data for the greater good[100].

Therefore, there is a **need to promote data integration and sharing of high-quality, harmonised, interoperable data**. Efforts need to be made to create awareness on how these contributions can advance research and lead to further innovation, or even breakthroughs, in improving health outcomes. Direct feedback may also motivate people to share data more routinely and altruistically. To ensure trust, data sharing should always be fair, transparent and non-discriminatory, and strong measures should be put in place to protect personal data and mitigate privacy risks for individuals. Industry should promote de-identification standards for research purposes and legislators should endorse best practices and standards[101].

As already shown in 1.3, data is the core of the digital transformation. Having access to a growing volume of data and being able to process it are both key to growth and innovation. **Data-driven innovation can deliver important benefits** for citizens and for the European economy, from refining decision-making to improving public services.

The European data strategy aims to make EU a leader in a data-driven society. Creating a single market for data will allow information to circulate freely within the EU and across all sectors for the benefit of businesses, researchers and public administrations. **The Communication on a European data strategy** adopted by the European Commission in February 2020 stressed that further EU actions could be taken **forward in a**

100 Cocir, European Health Data Space: Towards A Better Patient Outcome (2019)

101 Ibidem

Data Act, including to foster business-to-government data sharing for the public interest, support business-to-business data sharing, and evaluate the Intellectual Property Rights (IPR) framework with a view to further enhance data access and use.

In order to become an attractive, secure and dynamic data economy, the EU priorities are:

- Setting clear and fair rules on access and re-use of data;
- Investing in next generation standards, tools and infrastructures to store and process data;
- Joining forces in European cloud capacity;
- Pooling European data in key sectors, with EU-wide common and interoperable data spaces;
- Giving users rights, tools and skills to stay in full control of their data.

In May 2021, the Commission published its **Inception Impact Assessment on the forthcoming Data Act**[102]. This legislative initiative will aim at **facilitating data access and use and review the rules on the legal protection of databases**. The main purpose is to ensure fairness in the allocation of data value among actors of the data economy, including business-to-business and business-to-government situations. The Commission conducted a **public consultation, ending in September 2021**, on its Inception Impact Assessment, and gathered the views of all interested parties to shape the Data Act. Furthermore, in the European Parliament, the Industry, Research and Energy Committee (ITRE) adopted an initiative report on a European data strategy, which calls for the European Commission to submit legislation to foster data access and interoperability in the forthcoming Data Act. In parallel as already said in 1.3, **on 25 November 2020, the Commission unveiled its proposal for a Data Governance Act**[103].

The Regulation will empower users to stay in control of their data, and encourage the creation of common European data spaces in key sectors. These sectors include health, the environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.

To further ensure the EU's leadership in the global data economy **the European strategy for data intends to**:

- Adopt legislative measures on data governance, access and reuse. For example, business-to-government data sharing for the public interest;
- Make data more widely available by opening up high-value publicly held datasets across the EU and allowing their reuse for free;
- Invest €2 billion in a European High Impact Project to develop data processing infrastructures, data sharing tools, architecture and governance mechanisms to improve data sharing, and to federate energy-efficient and trustworthy cloud infrastructures and related services;
- Enable access to secure, fair and competitive cloud services by facilitating the set-up of a procurement

102 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en

103 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767

marketplace for data processing services and creating clarity on the applicable regulatory framework concerning the rules on the cloud.

Here, it is crucial to be aware that **governing health data for its secondary use is a distinct case in EU data governance**. Governing health data requires a specific mechanism and **cannot be governed by horizontal legislation alone**, such as the proposed Data Governance Act. There are many different reasons why health data needs *ad hoc* initiatives.

First of all, respect of a patient's right to protect personal data. With the General Data Protection Regulation[104] (GDPR), the EU has signaled the protection of personal health data as a fundamental right. Yet, aggregated health information consists of personal health data, with aggregated health information being essentially the basic input for research and policy-making. At the same time, **health data is special in that it regards a subject with high societal saliency** – that is, public health. The sharing of health data and the implied benefits for the wider public, could be the grounds on which the rights of an individual or patient may not prevail. This is clear in the case of infectious diseases, as well as societal or environmental health threats where the use of data is of vital and urgent interest, but also when developing prevention or treatment of other diseases. This requires the **balancing of various interests, especially public health and privacy**. These public health purposes create a good basis for the acceptance of the secondary use in communities. Cross-border sharing of data can markedly add to the power of data analysis and use.

Moreover, a **responsible secondary use of health data is imperative** to maintaining citizen trust and significant investments in data processing. Health data captured in professional systems and provided by citizens can be processed for secondary purposes, and both ways need specific cybersecurity management. Data subjects also need transparent information concerning how safe anonymisation or pseudonymisation are, while data controllers and data processors need up-to-date guidelines.

The growing volume of health data and **increasing variety of methods to use it** for secondary purposes is a growing source for the **development of new businesses and innovation** in personal health, health services, health care management, development of effectivity and quality of health services. National, regional and local health registries and Electronic Health Record (EHR) systems and the digitalisation of health build comprehensive options to use almost real-time data for industries – health app developers, health service providers, health and medical technology companies, ICT companies, pharma industry, insurers and healthcare platforms. **The GDPR allows for the use of data in the private sector for research purposes.** However, national health systems vary in Europe: from publicly funded systems, to semi-public health insurance and provision of health services, to totally private systems. The Data Governance Act separates governance mechanisms and rules for data from public or private sectors, but it does not specifically differentiate between

104 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434

health data provided by the public or private sector. The interests and usage of health data are different in private health services, pharma, health technology, ICT, or medical device industries.

To date, **many EU Member States have already established a national health data governance framework**, or are in the process of establishing one. Far fewer EU Member States, however, have embedded these nationwide and centralised regulatory frameworks for the access and reuse of health data in national law. As well, several Member States have reported experiencing **data governance challenges to developing health data infrastructures**, with most mentioning **legal or policy barriers to public authorities undertaking data linkages and sharing data** among public health authorities. Many institution-to-institution or within health sector procedures exist for the access to and exchange of health data (especially in country border regions where health institutions need to cooperate with cross-border institutions). These collaborations and (cross-border) exchanges of data may be governed by subnational regulations or even lower governance structures. This could lead to **fragmentation and hamper the unambiguous access and exchange of health data**, which, in turn, proves the need for a more unified regulatory framework.

The digital and data transformation initiative put forward by the European Commission in 2020 provides the springboard for the EU efforts to widen the use of data, including health-related data, in the future. This vision includes setting up a **European Health Data Space (EHDS) as a part of the European data policy**. The Member States have supported the proposal, which stems from the General Data Protection Regulation (GDPR). As mentioned above, the GDPR sets out many key concepts, such as health data being a special category of personal data as well as genetic and biometric data, which all need special protection. But there is also a broad body of other legislation relevant to the secondary use of health data. A specific feature in the field of health is that the **Member States have a margin to maintain or introduce further conditions** as regards the processing of health, genetic or biometric data, which may result in fragmentation.

The creation of a **European Health Data Space is one the key priorities of this Commission in the area of health**. The main purpose of the EHDS is to promote health-data exchange and support research on new preventive strategies, as well as on treatments, medicines, medical devices and outcomes. As a policy initiative, the EHDS aims to provide a common framework across EU Member States for the sharing and exchange of quality health data such as electronic health records, patient registries and genomic data.

In the Communication on the European Strategy for Data[105], the Commission announced its objective to **deliver concrete results in the area of health data** and to understand the potential generated by developments in digital technologies. The collection, access, storage, use and re-use of data in healthcare present specific challenges

105 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

that need to be addressed, as mentioned in the previous paragraph. This requires a regulatory framework that best serves individuals' interests and rights, especially concerning the processing of sensitive personal health data. Facilitating better access to and exchange of health data is essential to ensuring increased healthcare accessibility, availability and affordability. It will stimulate innovation in health and care for better treatment and outcomes, and encourage innovative solutions that make use of digital technologies, including AI.

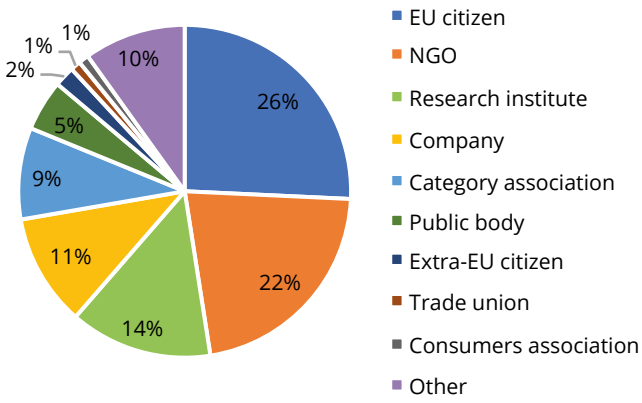
In mid-December 2020, the European Commission published its **Inception Impact Assessment on the European Health Data Space (EHDS)**. The document provides the context, the main objectives and problems that the EHDS aims to tackle, as well as policy options foreseen to meet the three core objectives. **The first goal presented by the European Commission** is to **ensure access, share and optimal use of health data** for healthcare delivery purposes as well as its re-use for research and innovation, policy-making and regulatory activities. **The policy options proposed are three**: the first is to establish a legal and governance framework to cover the access to and exchange of health data for healthcare provision, research, policy-making and regulatory activities; the second is to lower technical barriers hindering data use and re-use, in particular, those related to infrastructure, interoperability, data quality and standards in the health field; the third and last policy option involves ensuring the access and control of patients and citizens over their own health data. **The initiative's second objective is to foster a genuine single market in digital health** covering digital health services and products, including tele-health, tele-monitoring and mobile health. In this case, the policy option foreseen is to **remove barriers to the cross-border movement of digital health services and products**, including data-intensive ones, as well as to the rights of patients to benefit from those services and products, and their interoperability with electronic health records and healthcare systems. **The last objective**, as stated in the Inception Impact Assessment **is to enhance the development, deployment and application of trustworthy digital health products and services**, including those incorporating Artificial Intelligence (AI) in the area of health. In order to achieve this, the EC proposed to analyse liability rules related to the use of data-intensive services, including AI.

In May 2021, the European Commission launched an **open consultation, ending on 26 July 2021**, to gather stakeholders' opinions concerning the EHDS initiative. The consultation also aimed to **gauge what are the preferable policy options** for the implementation of the EHDS. It was split into three sections: access and use of personal health data, digital health services and products, and AI in healthcare. The following graph (Fig.2.3.1) represents the **percentage of respondents for each category**. Citizens participated more than any other category in the consultation, reaching **26% of the total**.

The platform for the cross-border exchange of patient data under the EHDS is planned to be operational in only **15 Member States by the end of 2021**. By **2023, however, 24 EU countries** (aside from Bulgaria, Austria

Fig. 2.3.1 Respondents to the open consultation on EHDS, by category

Source: European Commission



and Denmark) should be equipped for cross-border patient data sharing.

The European Health Data Space project will advance and accelerate the healthcare digital transformation, mainly by **ensuring that data is compatible and easily transferred**. The inevitable changes in current practices (e.g. IT system upgrades, new clinical pathways, etc.) will help make healthcare better, safer and more effective. In fact, the **European Health Data Space offers a vision, process and means to accelerate this transition**, before digital health technologies deliver their efficiencies, new knowledge and intelligence, and is a shift from care to prevention by improving disease prevention and early detection.

However, the EHDS should n**ot only be limited to the promotion of cross-border services or data transfers**. It should also address the broader issue of data access for permissible data use subject to appropriate safeguards, e.g. for research and innovation purposes, and not solely for the provision of care. Some of the issues medtech companies have been facing, above all regarding access to data in care delivery as well as research, **both relating to clinical research** (research on humans) **and non-clinical research** (on data, e.g. computer modelling and simulation), and re-use of health data, have their origin in different European legal frameworks. The legal basis chosen for the EHDS should allow for embedding this broader concept of data transfer.

Personalised healthcare has the potential to revolutionise patient care in the coming decades. To a great degree, it already has, but a truly transformative healthcare system needs a robust, unified and secure bank of data. A wealth of data is already out there, but the public and private sector will need to work together to seize the opportunity to create an EU Health Data Space.

Following the Inception Impact Assessment and the consultation, **many organisations have commended the initiative and decided to share their opinions on the EHDS**. The respondent organisations stressed that many issues, from the **paramount issue of data governance and the crucial role of interoperability**, to the flexibility of the legal framework to future data sources and technology are key to the success of the initiative. Furthermore, European citizens must feel that their data is secure and **being used with a positive healthcare intent**. For this reason, simple clear language and available education tools will be required for universal

trust in and use of data. To create a positive environment for health data in Europe there will need to be a focused political leadership, as well as technical expertise.

More issues arise varying from **insufficient health data exchange for healthcare service provision** (as a result of under-investment and lack of political leadership in making it a priority) and **fragmentation of digital standards**, to **limited digital interoperability between healthcare systems** and the need for all Member States to align the **assessment procedures and criteria that digital products or services need to meet to be eligible for reimbursement**, and to overcome fragmentation. Since aligning incongruent national strategies through an EU-wide governance framework will enable Europe to harness the power of health data in a resource-and cost-effective way, such a framework should include, first of all, benefits for citizens. In fact, if the benefits are real, and the regional and national initiatives for personal data space meet citizen needs, **trust will follow**. Other success factors are the need for a coordinated interpretation of the GDPR among Member States and the **respect of intellectual property required for companies to access data**. Furthermore, achieving technical and semantic interoperability and the seamless exchange of data and information is key to the success of the European Health Data Space and improvements in clinical operations, patient outcomes and healthcare costs. Lastly, digitalisation places demand on **healthcare professionals (HCPs) who are required to adapt and update their clinical competences**, which involves the necessary, but not always straight-forward understanding, of how AI solutions can match their needs and enhance their medical practice. Promoting professional education and training in digital literacy for healthcare professionals should be an integral part of the policy agenda, taking into account both university education and lifelong learning programmes.

PART 3 ENERGY

3. ENERGY

3.1. THE EUROPEAN UNION AND THE ENERGY TRANSITION

3.1.1. The EU in the global decarbonisation scenarios

Global energy demand reached 13,297 Mtoe in 2020, a 10% increase compared to 2010. The growth was mainly driven by consumption in the Asia-Pacific area, that increased by almost 29% compared to 2010 (Fig. 3.1.1). On the other hand, this increase was offset by the lower consumption of the United States (-5.5%) and, above all, of the European Union (-14.3%) which, with its 1,332 Mtoe, ended up representing, in 2020, one tenth of the world consumption of primary energy, 3 pp less than ten years earlier (Fig. 3.1.2).

The European Union is also the only region with the largest share of renewables in the energy mix with 13% in 2020, clearly above the world average, at only 6% (Fig. 3.1.3). The US has a share only slightly above

Fig. 3.1.2 Final energy consumption (%)

Source: BP Statistical Review of World Energy 2021

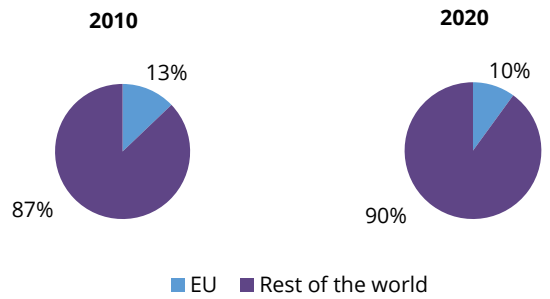
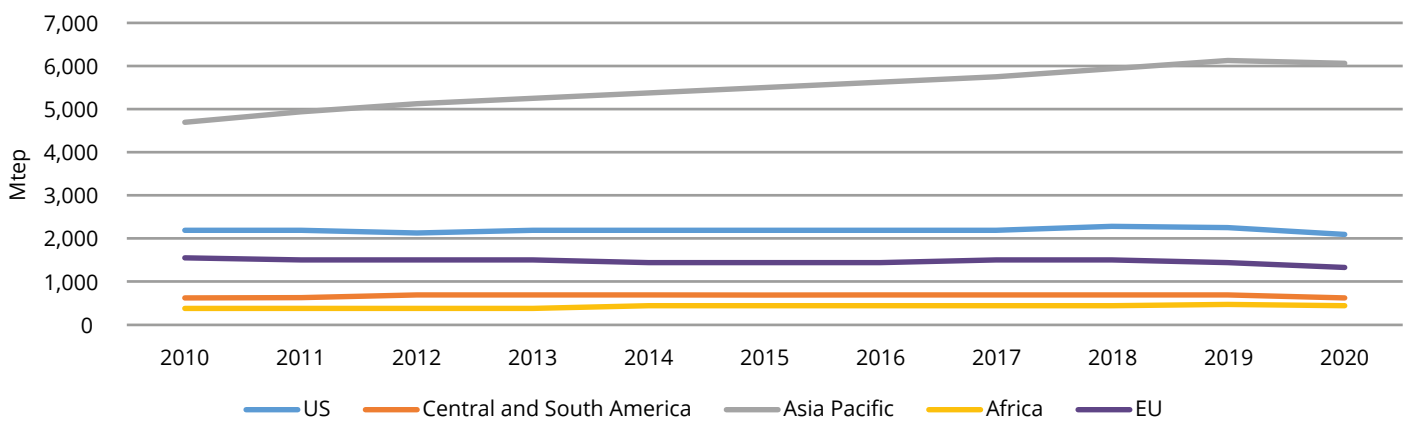


Fig. 3.1.1 Primary energy consumption

Source: BP Statistical Review of World Energy 2021



the global average (7%), while oil is still important, and dominant, representing over one third of US primary energy (37%), more or less in line with the EU (36%). The Asia-Pacific area, on the other hand, mainly relies on coal, which accounts for about one half of the total primary energy.

According to data released by IRENA (International Renewable Energy Agency), Western Europe ranked second for investments in renewables in the period from 2013 to 2018 amounting to $347 billion, 19% of the world total (Fig.3.1.4). The installed capacity from renewable sources increased from around 303 GW in 2011 to over 528 GW in 2020, registering an increase of +74% compared to only 10.5% globally (IRENA, Renewable Energy Statistics 2021). Future scenarios also promise further important steps forward as renewable energies are increasingly becoming the cheapest source of electricity in many markets. Therefore, investments are destined to grow and, with them, the installed capacity which, according to IRENA forecasts, will rise from33% in 2017 to 69% in 2050, in the so-called "Planned Energy Scenario", i.e. a scenario based on current policies and plans, and even 91%, in the "Transforming Energy Scenario", which envisages the ambitious goal of limiting the increase in the global average temperature to +1.5°C, compared to pre-industrial levels, by the end of this century (Fig. 3.1.5). Similar scenarios are for the EU which has an already better starting point, with already almost half of the installed capacity from renewable sources in 2017.

Fig. 3.1.3 Energy mix, by region (2020)

Source: BP Statistical Review of World Energy 2021

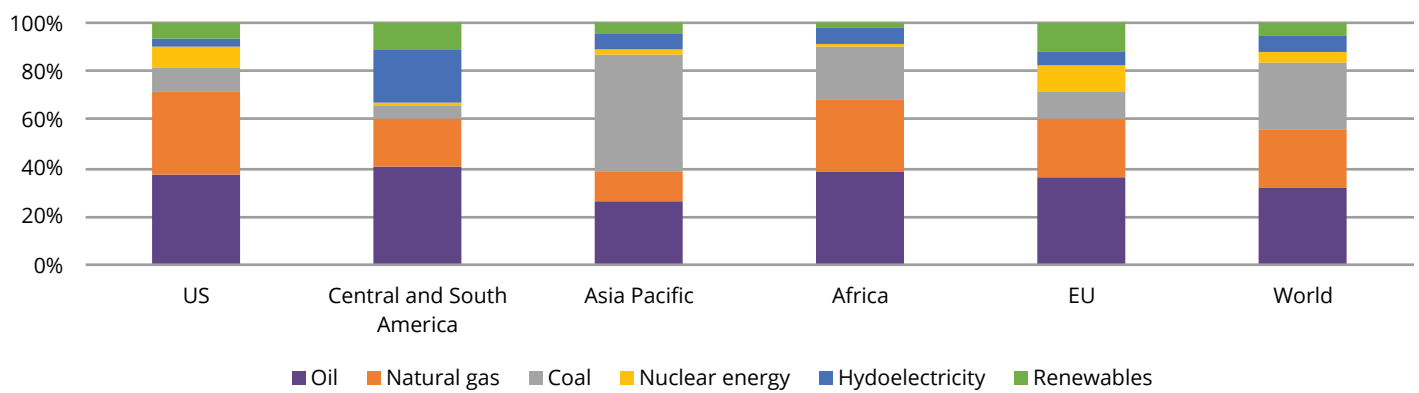


Fig. 3.1.4 Renewables investments (2013-2018)

Source: IRENA

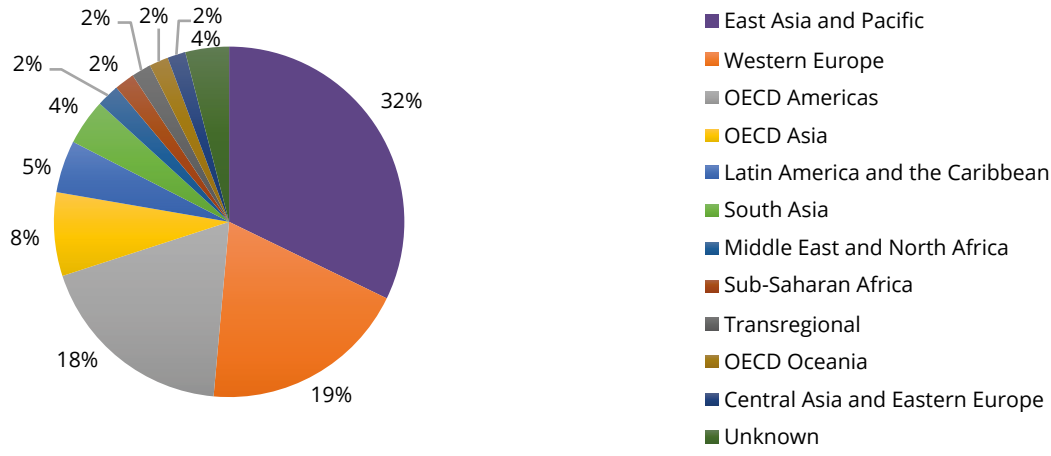
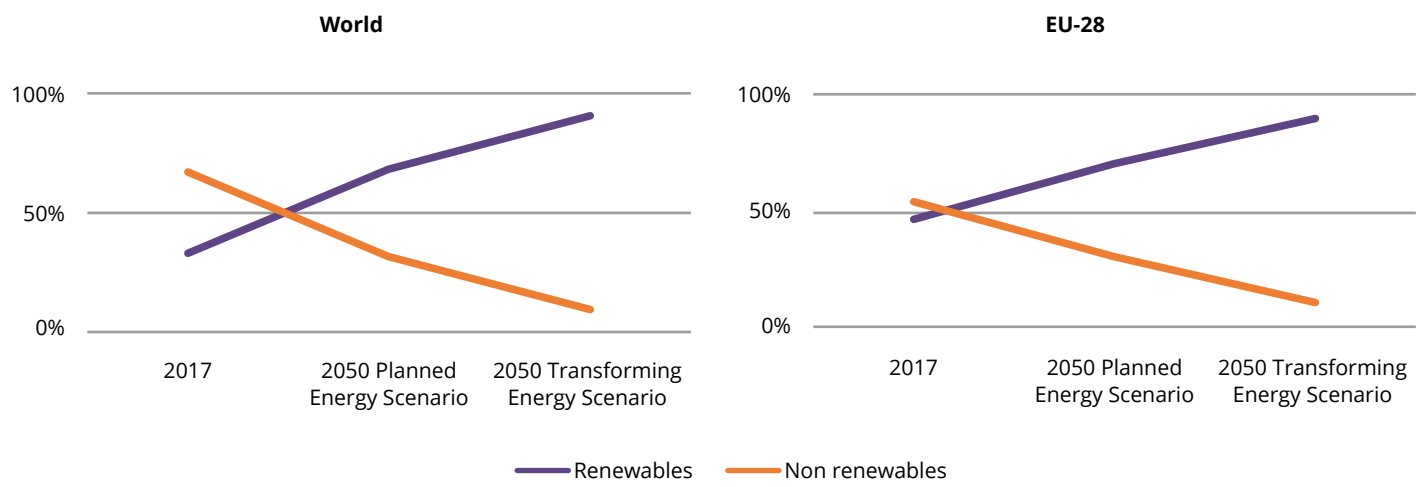


Fig. 3.1.5 Installed capacity from renewable energy sources: future scenarios

Source: IRENA



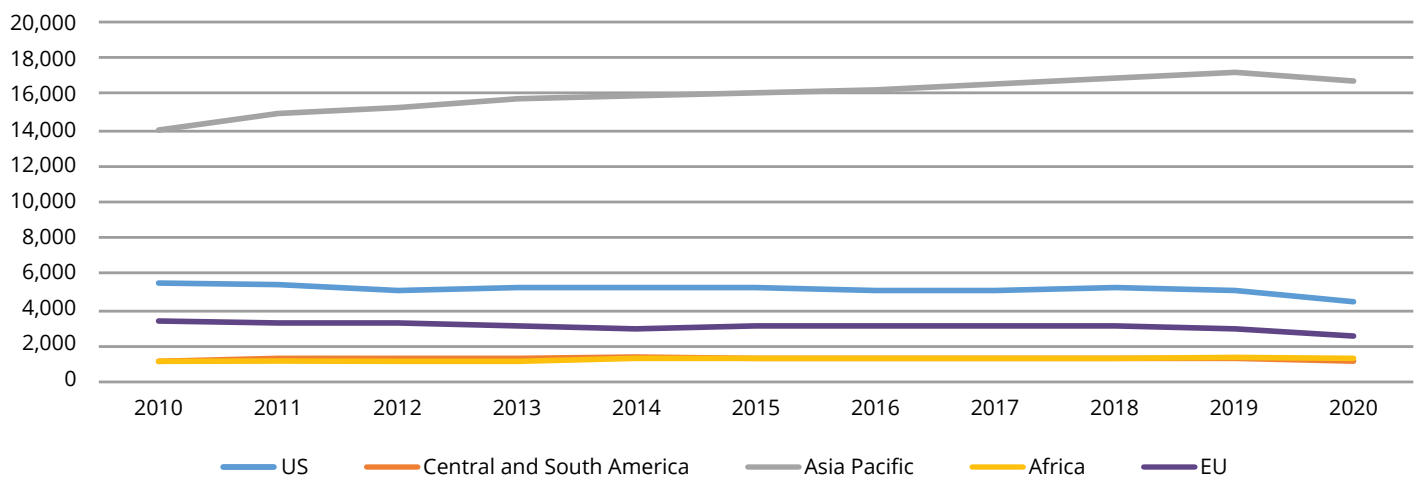
In line with the increase in consumption, globally produced CO_2 emissions have also increased, albeit proportionally less (+3.2%) – from 31,291 Mt in 2010 to 32,284 Mt in 2020. Also in this case, the increase is mainly due to emissions from the Asia-Pacific area, which increased by about one fifth over the decade, and secondarily to those produced in Africa (+7%). While the US and the EU contributed with a considerable decrease to the decarbonisation objectives – -18.9% for the former, -24.7% for the latter (Fig. 3.1.6). However, it is worth noting that, when compared to the population, the US contribution to global emissions is much higher – about 13.46 Mt per capita, compared to just under 4 Mt per capita in the Asia-Pacific area, 5.7 Mt in the EU and a global average of 4.14 Mt.

3.1.2. The European Green Deal and Next Generation EU

Article 191 of the Treaty on the functioning of the European Union places the protection and improvement of environment quality among its main objectives. By virtue of this principle, over the years, the Union has adopted numerous measures to reduce the impact on the ecosystem of human activities and combat climate change. In order to promote zero emissions and support Member States in their path towards a fair and inclusive transition, in December 2019, the European Commission presented the ambitious communication on the European Green Deal. The strategy aims at making energy production and European citizens' lifestyle more sustainable and less harmful to the environment. The Green Deal is divided

Fig. 3.1.6 CO_2 emissions (Mt)

Source: BP Statistical Review of World Energy 2021



into a series of macro-actions containing strategies for all sectors of the economy and, in particular, transport, energy, agriculture, construction and industrial sectors such as steel, cement, Tlc, textile products and chemicals. It also includes a series of measures of different nature, including, above all, new regulatory provisions and investments, to be implemented over the next thirty years. At the same time, the Commission has launched a European Green Deal Investment Plan (EGDIP), mobilising up to €1 trillion.

The strategy is made up of **eight main objectives**:

1. Making the EU climate goals for 2030 and 2050 more ambitious;
2. Ensuring the supply of clean, economical and safe energy;
3. Mobilising industry for a clean and circular economy;
4. Building and renovating in an energy and resource efficient way;
5. Accelerating the transition to sustainable and intelligent mobility;
6. "From producer to consumer": designing a fair, healthy and environmentally friendly food system;
7. Preserving and restoring ecosystems and biodiversity;
8. "Zero pollution" for an environment free of toxic substances.

Since March 2020, the initiatives taken by the Commission have been numerous. These are mainly action plans and strategic documents concerning the multiple areas included in the European Green Deal. Among these, a prominent place is held by the European Climate Law, aimed at inserting into **EU law** the goal of climate neutrality by 2050, which in turn has 4 objectives:

1. to establish the long-term direction period for achieving the climate neutrality goal by 2050 through all policies, in a socially fair and cost-effective way;
2. to create a progress monitoring system and take further action if necessary;
3. to provide for conditions of predictability for investors and other economic actors;
4. to ensure that the transition to climate neutrality is irreversible.

To this end, the 2030 Climate Target Plan was prepared, setting a new greenhouse gas reduction target for 2030 (at least 55% compared to 1990 levels), and stimulating the creation of green jobs and encouraging international partners to be more ambitious in containing global warming by limiting global temperature rise to 1.5 °C.

The EU will also provide for financial support and technical assistance to help those most affected by the transition to the green economy. This is the so-called Just Transition Mechanism, which will help mobilise at least €100 billion for the period 2021-2027 in the most affected regions, through:

1. a new Fund for a just transition of €40 billion, generating investments for €89-107 billion;
2. an InvestEU "just transition" scheme aimed at mobilising €30 billion in investments;
3. an EIB public lending facility of €10 billion in loans that should leverage up to €30 billion in investments.

Member States are not unprepared for this challenge. Over the last few decades, EU countries have increasingly

invested in green technologies and in the production of energy from renewable sources. In 2019, renewables represented 13.6% of EU total gross domestic consumption (Fig. 3.1.7). The most virtuous country is Sweden (30%), followed by Latvia (28.2%) and Finland (26.3%). Italy with 16%, (2.4 p.p. more than the EU-27 average) ranks tenth in terms of the share of renewables in gross domestic consumption.

Among renewable energy sources, sun and wind energy carry the greatest weight in the European race towards climate neutrality. The installed electricity production capacity from these two sources amounted to approximately 289 GW in 2019 (Fig.3.1.8). Germany takes the lion's share, with 190.8 GW (66% of EU installed capacity), a value of over five times higher than Spain (36.9 GW), ranking second. Italy, with 31.5 GW installed, ranks third, ahead of France (27.9 GW) and the Netherlands (12.2 GW).

Another essential dimension for the challenge of decarbonisation, as well as for strengthening the security of supply, is energy efficiency. Here, it is useful to look at internal energy consumption (Fig. 3.1.9). The country that consumes the least energy per unit of GDP is Ireland (0.49 GWh per € million), followed by Denmark (0.65) and Malta (0.75). Italy, despite being one of the main manufacturing economies in Europe, consumes 1.01 GWh per € million of GDP produced, less than France (1.20), Spain (1.19) and Germany (1.02).

In order to steer the economic recovery in the green direction, in February 2021, the regulation relating to the Recovery and

Fig. 3.1.7 Renewables share out of total gross internal consumption (2019)

Source: Eurostat

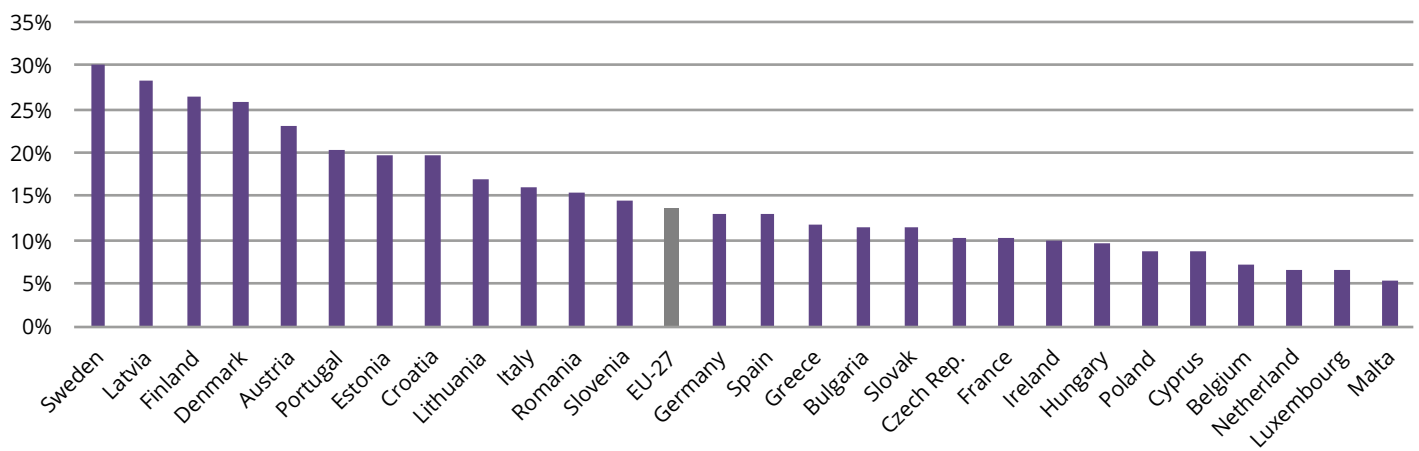


Fig. 3.1.8 Installed capacity of wind and solar photovoltaic energy production (GW, 2019)

Source: Eurostat

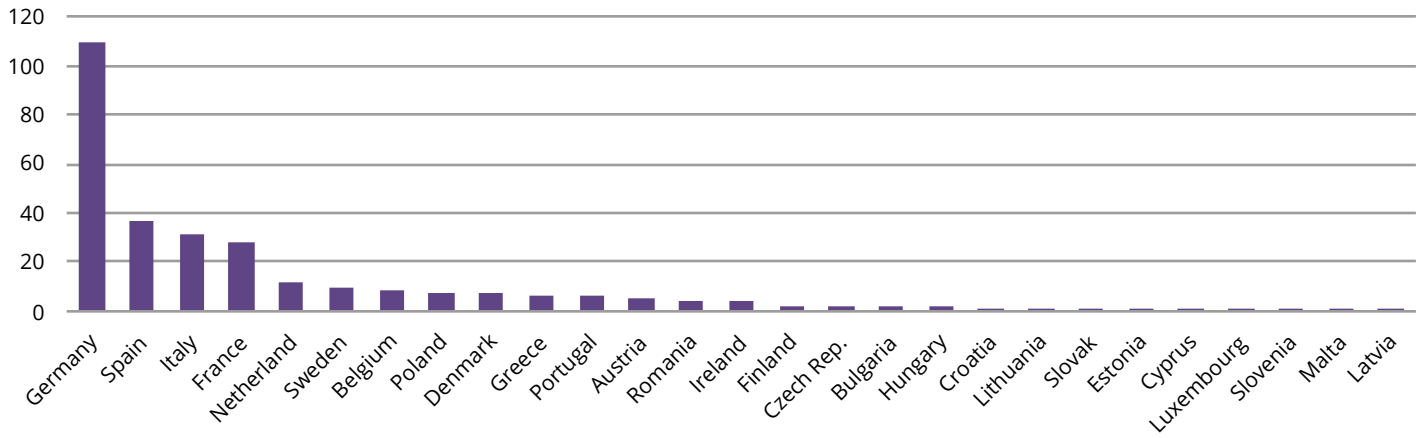
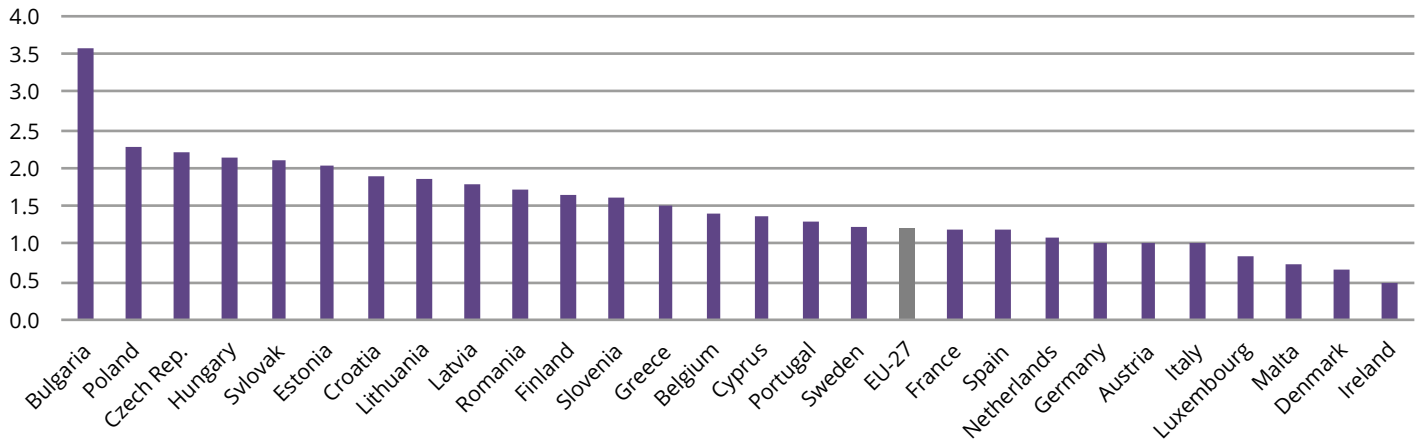


Fig. 3.1.9 Gross internal consumption on GDP (GWh/M€, 2019)

Source: Eurostat

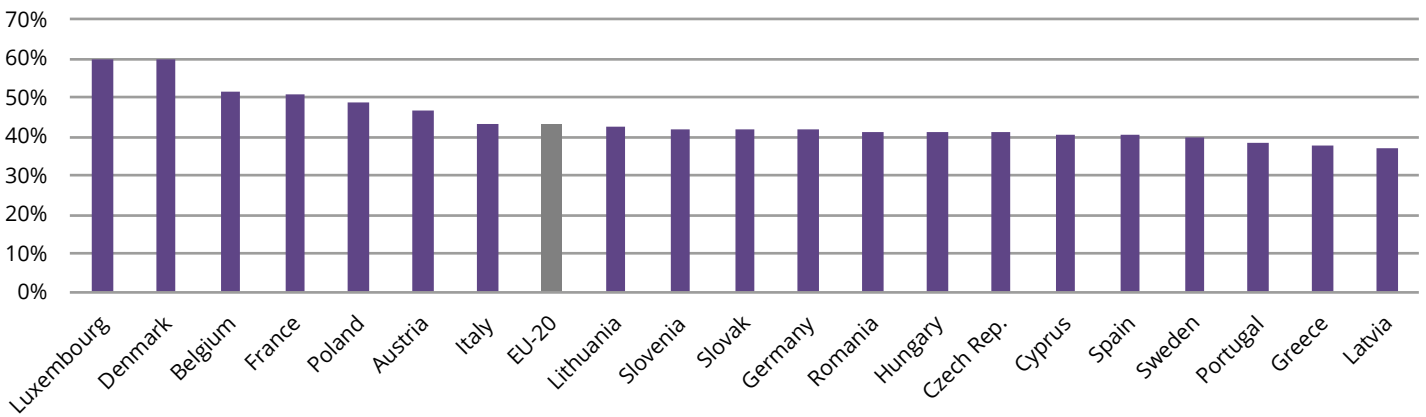


Resilience Facility (RRF) was published. This is the key tool of the Next Generation EU package which aims at mitigating the economic and social impact of the Covid-19 crisis and, at the same time, addressing the long-term challenges of the Union. The RRF provides for a disbursement of resources for €723.8 billion divided into grants (with a ceiling of €338 bln at current prices) and loans (€385.8 bln).

One of the main conditions imposed by the EU is that the plans drawn up by the MSs contribute substantially to the green transition, as promoted by the Green Deal, and that, therefore, at least 37% of the available resources should be assigned to the green compartment. According to a comparative analysis of the National Plans presented to the Commission, the country that has devoted the largest share of its funds to the ecological transition is Luxembourg (60% of the available resources) (Fig. 3.1.10), followed by Denmark (59.6%) and Belgium (51.7%)[106]. Italy, which is the main beneficiary of the RRF (€191.5 bln), has diverted 43% of available resources to the ecological transition and environmental sustainability, in line with the EU average[107].

Fig. 3.1.10 Share of resources of MS NRRPs devolved to environmental sustainability

Source: Bruegel



106 "European Union countries' recovery and resilience plans", Bruegel (https://www.bruegel.org/publications/datasets/european-union-countries-recovery-and-resilience-plans/), based on what was declared by MSs. A third party survey probably attains to different outcomes (the different evaluations from green trackers about the contribution of NRRPs for the purpose of ecological transition).

107 The first 20 countries that presented their own National Recovery and Resilience Plan are considered.

The investments and reforms proposed in the National Recovery and Resilience Plans also need to comply with the "Do no significant harm" (DNSH) principle, pursuant to the European regulation on the taxonomy for sustainable activities. The latter is a tool helping investors, companies and project promoters lead the transition to a low-carbon, resilient and resource-efficient economy. The taxonomy establishes the performance thresholds ("Technical screening criteria") for economic activities that:

- make a substantial contribution to one of the six environmental objectives[108];
- do not cause significant damage (DNSH) to the other five;
- meet minimum guarantees (e.g., OECD Guidelines on Multinational Enterprises and United Nations Guiding Principles on Business and Human Rights).

The Commission then published a guide to the implementation of the second of these principles outlining the key principles and a two-step methodology for the evaluation of "Do no significant harm".

First of all, the document defines when an activity involves significant damage, in relation to each of the six objectives. The Commission has also prepared a checklist that guides national governments in analysing how each measure stands with respect to DNSH. The checklist is based on a two-step procedure that must be activated for each project envisaged by the National Recovery and Resilience Plans. The procedure, thus, distinguishes between measures that do not cause foreseeable damage for any of the objectives outlined – and for which, therefore, a simplified approach is sufficient – and those that require a substantial DNSH assessment.

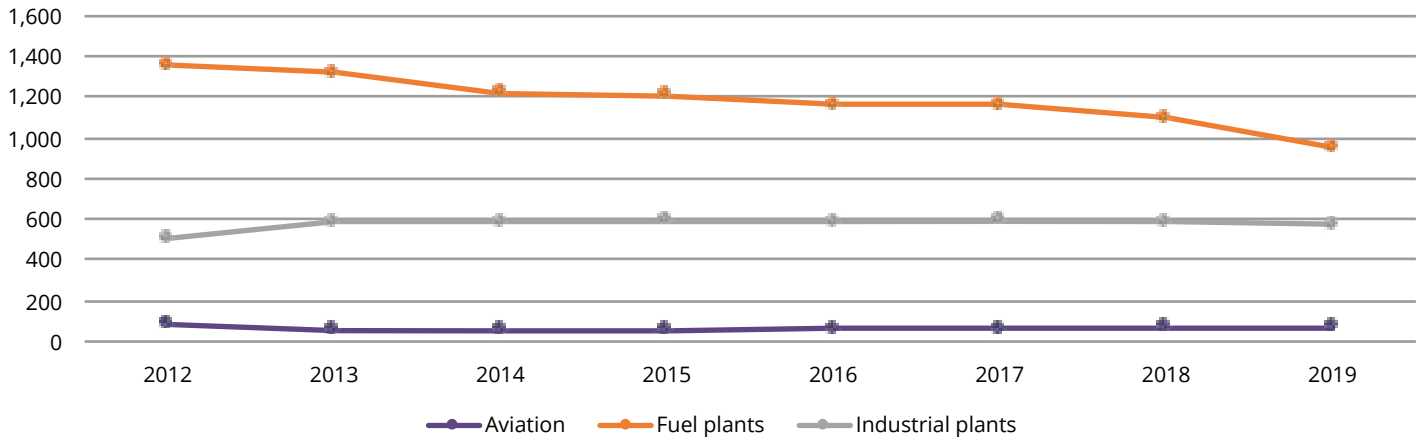
108 The six objectives are: climate change mitigation; adaptation to climate change; protection of water and marine resources; transition to a circular economy; pollution prevention and control; protection and restoration of biodiversity and ecosystems

3.1.3. Fit for 55: the reform of European energy and climate policies

Reducing emissions is the main objective of EU policies. To this end, the Emissions Trading System (ETS) was launched in 2005 and, today, it is one of the cornerstones of Community policies. It has undergone various revisions (phase 4 of the programme runs from 2021 to 2030) and has expanded the number of countries involved and sectors and plants covered. If we consider the current scope of the ETS, data from the European Environment Agency shows that verified emissions from stationary installations (thus, excluding aviation) decreased by 35% between 2005 and 2019, decreasing at an annual average rate of about 3%, to reach 1.53 Gt CO_2 equivalent. By restricting the reference timeframe starting from 2012, when aviation was included in the ETS, it should be noted that combustion plants have reduced their emissions the most. In fact, between 2012 and 2019 they reduced emissions by 30%, despite still accounting for 60% of the total verified emissions. Industrial plants (from oil refining to the production of iron, aluminum, glass, ceramic, paper, etc.), on the other hand, have increased their emissions, on average, by 14% and account for 36% of overall emissions. Aviation, which accounts for 4% of emissions, reduced them by 19% (Fig. 3.1.11).

Fig. 3.1.11 Emissions by ETS sector (Mt CO_2 eq.)

Source: I-Com elaboration on data from the European Environment Agency



Industrial plants have also benefited, especially in the first two phases of the ETS, from free permits to a larger extent relative to their own emissions. On the other hand, European industry is facing energy prices that are on average higher than competitors in other regions of the world. Trinomics data shows that the weighted average price of electricity for industrial uses is higher in the EU-27 than in China and the US (but lower when compared to Japan). The price of gas, on the other hand, is higher than in the US, but lower when compared to Japan and China. Furthermore, electricity and gas prices for European industry are higher than the average for the G20 countries. It is clear how, in this field, the climate protection objectives are intertwined with the need to not jeopardise the competitiveness of the continental production system vis-à-vis the major global players.

The ETS reform is, therefore, one of the pillars around which "Fit for 55" revolves. It is the package of measures proposed by the European Commission, aiming at placing the EU on the path to reducing CO_2 emissions by 55% by 2030, the first step towards achieving climate neutrality by 2050. "Fit for 55" consists of 16 acts – two communications, four directives, eight regulations and two decisions. The communications concern emission targets for the coming decades and infrastructures for alternative fuels. The directives concern the ETS, renewable sources, energy efficiency and the taxation of energy products and electricity. The regulations relate to Effort Sharing (the annual reduction targets of emissions by the States of the Union), the carbon adjustment

mechanism at the border (CBAM), the creation of a Social Climate Fund, the use of soil and forestry (LULUCF), emission standards for cars and vans and infrastructure for alternative fuels, through the revision of the DAFI, air transport (ReFuelEu Aviation), and the use of renewable and low-carbon fuels in transport maritime (FuelEu Maritime). The decisions also propose a notification system for emission offsets for the aviation sector and the ETS market stability reserve until 2030.

Overall, in this way, the European Commission wants to review the entire toolbox available to climate policies, setting the bar high for ambitions. The imagined measures are numerous. With regard to the ETS reform, it is proposed to increase the emissions cut by 2030 from 43% to 61% when compared to the 2005 level. In addition, the maritime transport sector is included in the ETS, while for road transport and the residential sector it is intended to establish a separate ETS starting from 2025. Air transport, on the other hand, will gradually reduce free emission permits. In general, the free assignments of ETS permits will decrease as the CBAM becomes fully operational, i.e. the mechanism aimed at combating carbon leakage phenomena and whose implementation is closely linked to the application of the ETS. In order to prevent the leakage of emissions, EU importers will be required to purchase certificates corresponding to the cost of CO_2 that would be borne by the products if they had been produced within the Union. The price of the certificate will be equal to the average CO_2 price defined by the ETS auctions. CBAM will weigh in from 2023 on imports of cement, electricity, fertilizers, steel, iron and aluminum.

As for the sectors that are not included in the ETS, the target of reducing emissions by 2030 increases from 29% to 40%. Similarly, effort sharing provides for an increase in obligations for MSs. Furthermore, a significant use of the "carbon sink" by the countries of the Union is envisaged. The EU states will have to achieve climate neutrality in agriculture, land use and forestry by 2035. In relation to the production of renewable energy, the "Fit for 55" package increases the target to 40% by 2030 and, as part of the energy efficiency, primary consumption is expected to drop by 39% and final consumption by 36%, with an annual reduction rate for EU countries that has almost doubled. The goals envisaged for the mobility sector, according to which car and van emissions should be brought to 0 by 2035, are particularly challenging. At the same time, a decisive development of recharging and refueling networks is proposed. Specifically, an additional 1 kW of charging capacity is required for each electric car registered and a 600 kW system every 60 km along motorways. For hydrogen refueling, a site is imagined every 150 km. The structure of the energy taxation (Energy Taxation Directive) is also revised, parameterising it to the actual energy content and environmental performance. For these reasons, the highest minimum level is established for petrol and diesel. The lowest level is set for electricity, green hydrogen, advanced biofuels and biogas. In the intermediate range are methane and LPG. The Social Climate Fund will also be operational from 2024, financed until 2032 with €144 billion, partly obtained from the proceeds of the ETS for road transport and

buildings. It aims at reducing the economic impact on consumers resulting from the new emission reduction measures. Each EU country, in order to access the fund, will have to submit to the Commission a plan that includes measures to support citizens at risk of energy poverty and businesses exposed by the ETS reform. At the same time, the allocation of funds for innovation is increased.

For this reason, to access it, each country will have to submit to the Commission a plan including measures in favour of companies exposed to the ETS reform and citizens at risk of energy poverty. The measures advanced by the Commission immediately sparked off an intense public debate. On the one hand, there are numerous doubts about the impact of the measures on consumers and businesses, the effects on the competitiveness of European industry, the ability to quickly make the investments necessary to support the envisaged decarbonisation path, just to name a few. On the other hand, there are those who believe that the objectives set are still inadequate for the path to climate neutrality. Certainly, the contents of the "Fit for 55" package, which, we recall, are proposed by the Commission, are the subject of an intense debate among MSs and will have to be examined by the Council and Parliament, before a definitive go-ahead.

3.2. THE ROLE OF GREEN FINANCE ON THE ROAD TO DECARBONISATION

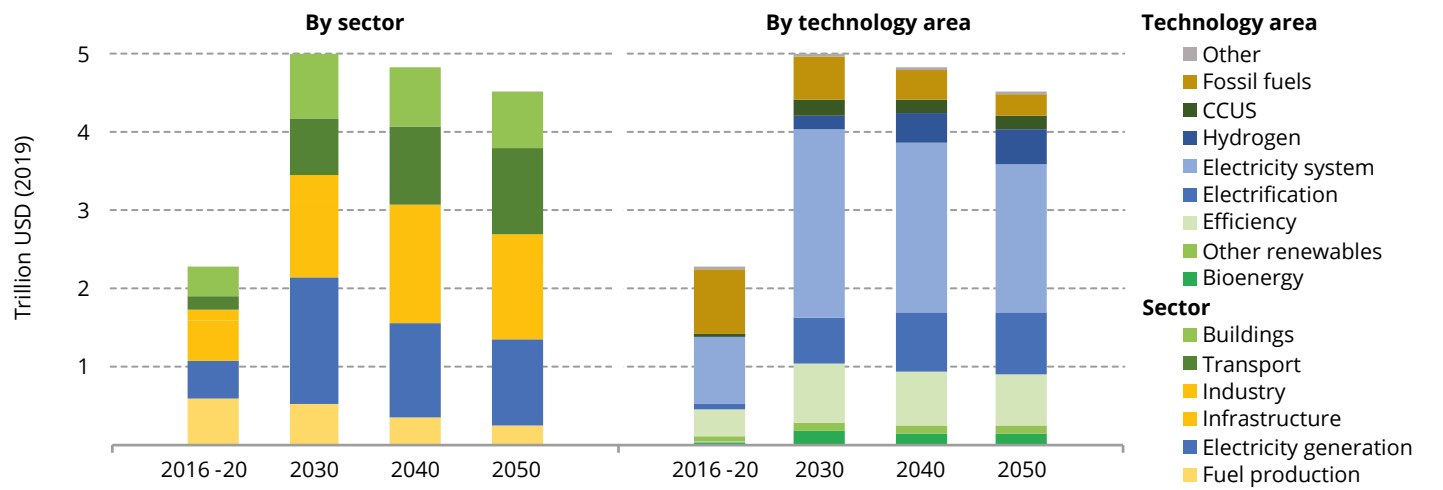
3.2.1. The relationship between the international financial system and ecological transition

The most recent scenario analyses highlight the need to mobilise a considerable amount of funding to achieve the goal of climate neutrality by 2050. The IEA report "Net Zero by 2050: A Roadmap for the Global Energy Sector" quantified US $5 trillion by 2030 as the investment needed for the energy transition, about 4.5% of global GDP. After 2030, the funding for decarbonisation should then be reduced, maintaining a level of around 4.5 trillion by 2050 (Fig. 3.2.1).

Today, investments to achieve climate neutrality are much lower than what is needed. In 2020, global investments in the low-carbon energy transition amounted to $501.3 billion[109], up from $458.6 billion last year and from just $235.4 billion in 2010 (Fig. 3.2.2). The first sector for investments has been renewable energy ($303.5 billion), up by 2% compared to 2019 despite some delays due the Covid-19 pandemic. Following, we

Fig. 3.2.1 Annual average capital investment in the Net Zero Emissions Scenario

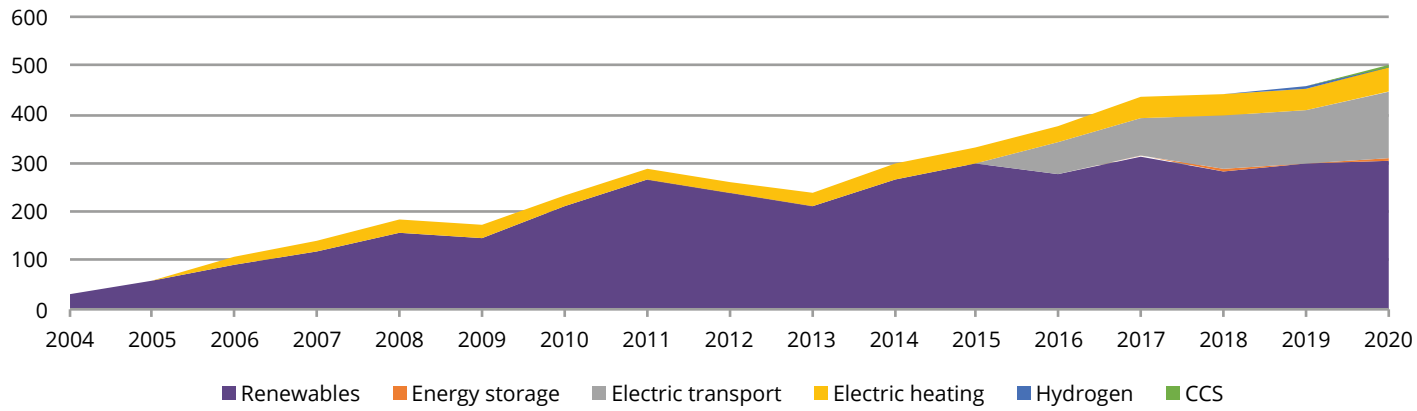
Source: IEA, Net Zero by 2050 A Roadmap for the Global Energy Sector



109 This includes investments in projects, such as renewable energy, energy storage, electric vehicle charging infrastructures, hydrogen production and CCS projects, as well as end-user purchases of low-carbon energy devices, such as solar systems on a small scale, heat pumps and zero-emission vehicles.

Fig. 3.2.2 Investments in the energy transition (bln $)

Source: BNEF



find electric transport with $139 billion being invested in new vehicles and charging infrastructures (+28%) and electric heating with $50.8 billion in investments (+12%), while hydrogen and CCS are marginal (1.5 billion and 3 billion, respectively), but expected to grow, however, in the future.

Europe and China are currently competing for the most active markets in energy transition investments. Last year, European countries allocated a large part of the increase in investments in this area. Growth for Europe is +67% compared to 2019, for a total value of $166.2 billion, higher than China and the US.

In the broader framework of sustainable finance, an essential factor is green bonds. These are bonds that, on the one hand, offer financial returns on a par with any other bond and, on the other, guarantee returns in environmental terms as they finance activities and projects with positive effects on the environment. Green bonds help bridge the gap between providers of capital and green goods, helping governments raise money for projects that aim to achieve climate goals and enabling investors to achieve sustainability goals. Together with other innovative capital market tools, green bonds support new or existing green projects through access to long-term capital. A green bond, therefore, like conventional bonds, supports the issuer of the bond in raising funds for specific projects in exchange for the payment of a fixed periodic interest and a full repayment of the principal at maturity. A green bond, however, has a "green" label, which tells investors that the funds raised will be used to finance environmentally beneficial projects. The definition of the right criteria and standards

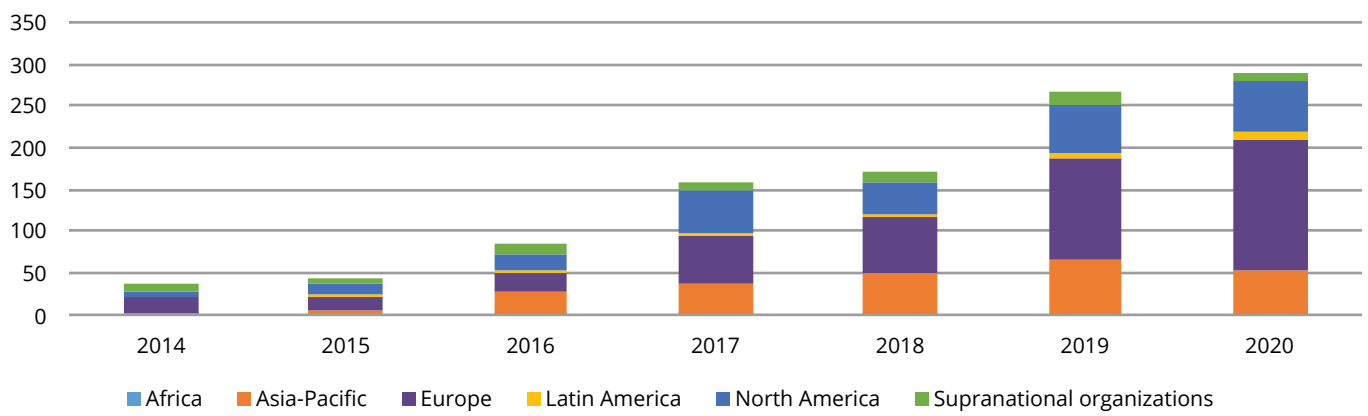
for assigning the "green label" is essential to ensure that sustainable finance promotes the energy transition.

The green bond market emerged about a decade ago and has experienced rapid growth since then, particularly in recent years. According to data released by the Climate Bonds Initiative, one of the main international organisations engaged in mobilising and orienting the capital market towards solutions to combat climate change, 2019 was the first year since 2016 in which all regions of the world recorded an increase in green bonds issued, also with considerable variations. Europe recorded the largest increase, with $50 billion more than in 2018, accounting for as much as 57% of global expansion. In 2020, after a first quarter of strong growth, green bond issuance clearly suffered from the pandemic in the second quarter, but a record third quarter ensured a good overall result. The value of the green bonds issued increased by a further 8.8%, reaching $290 billion (Fig. 3.2.3). Europe recorded a growth of 28% at the end of the year, with an overall increase (+$34.5 bln) even higher than the world average (+$23.2 bln), which was instead affected by the decline recorded in the Asia-Pacific area (-$12 bln) and by supranational organisations (-$4 bln). This trend strengthens European leadership, with an overall volume, in the 2014-2020 period of approximately $465 billion, almost double that of North America and the Asia-Pacific area. From the first data relating to 2021, green bonds issued amount to $124 billion.

From a market initially dominated by non-financial companies and development banks, the green bond market has recorded growth not only in terms of the

Fig. 3.2.3 Investments in green bonds, by geographical area (bln $)

Source: Climate Bonds Initiative



amount issued, but also in terms of diversification of the type of issuers (Fig. 3.2.4). Although the value of green investments has sharply increased, from $9.3 billion in 2014 to almost 40 in 2020, the incidence out of the total of non-financial companies has halved (from 51.4% to 25.5%). Investments by development banks, which increased from $4.8 to 13.3 billion, represented, in 2014, 26.5% of the total, while, in 2020, only 8.5%. On the other hand, financial companies have gained ground which, with $31.2 billion invested in 2020 (up from only 0.8 bln six years earlier), make up for exactly one fifth of the green bonds issued. The weight of state-supported entities has also been increasing, rising from 10% to 25%, with bonds issued for about $39 billion. Then, starting from 2016, ABS companies (Asset-Backed Security) and green bond loans made their entry. However, by 2020, they still only held a very marginal share (1.5%), while green sovereign debt was more successful, growing from $0.8 billion in 2016 to $28.5 billion in 2020. It now represents almost a fifth of the market.

Furthermore, the situation has also changed regarding the sectors financed (Fig. 3.2.5). In 2014, more than half of the green bonds were aimed at the energy sector, while in 2020, they appeared to be much more evenly distributed. Although it remains the predominant sector, the share of the energy market fell from 52% to 36% in the period, while residential (+6 p.p.) and transport grew significantly, doubling out of the total .

The success of green finance is also highlighted by the performance of the clean energy shares. According to Carbon Tracker, from 2012 to 2020, the shares issued on the stock exchange by fossil fuel producers (for a

Fig. 3.2.4 Green bonds issued, by type of issuer (%)

Source: Climate Bonds Initiative

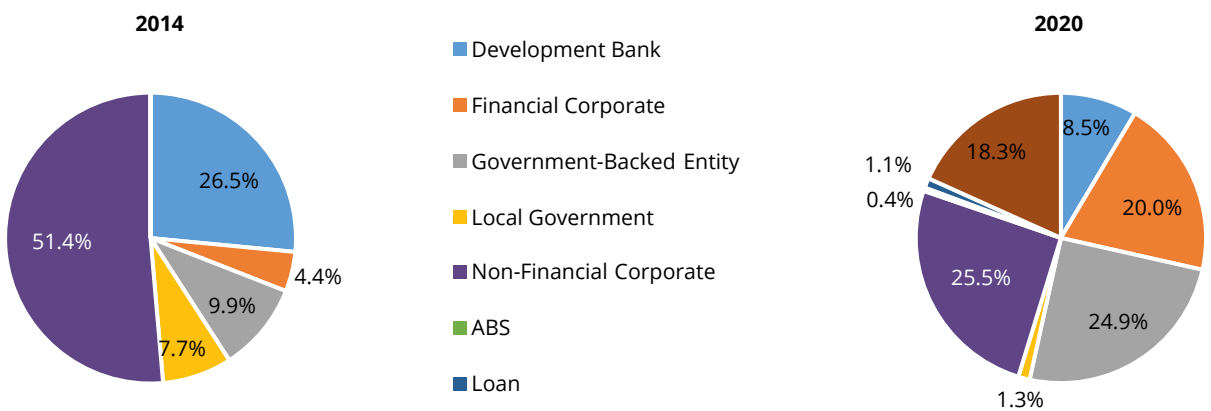


Fig. 3.2.5 Green bonds issued by funded sectors (%)

Source: Climate Bonds Initiative

total of $453 bln) ended up losing $123 billion in value and their performance was much lower than the "MSCI All Country World Index", a general market index taken as a reference by Carbon Tracker analysts. The biggest loss was recorded in the Oil and Gas segment (-$85 bln). On the contrary, in the same period, the value of the stock market transactions carried out by electric utilities increased by $119 billion in absolute terms, while the value of the shares issued by clean energy companies increased by $77 billion, with a performance of more than 50% higher than the MSCI World Index. According to Bloomberg NEF's analysis, stocks in the clean energy sector, which for much of the last decade had not performed well, gained appreciably in 2020. This triggered a turnaround that led to a growth in prospects for wind and solar energy and electric vehicles. Investors were motivated by the increase in the cost-effectiveness of green actions compared to those of fossil fuels, by the expectation for a "green recovery" from the Covid-19 recession and by the probable launch by the Biden administration of a low-carbon policy in the US.

In the international financial system, central banks also turned their attention to sustainability issues. In 2017, the Network for Greening the Financial System was set up. It is a global network of central banks and supervisory authorities aimed at sharing good practices and formulating recommendations regarding the management of environmental and climate risks in the economic and financial fields. There are numerous areas for central banks to take action – from the definition of climate scenarios useful for monetary authorities to conducting stress tests to the integration of climate risks

in the assessment of creditworthiness, to the definition of suitable metrics and indicators for the inclusion of sustainability criteria in investment choices.

3.2.2. European policies for the financing of sustainable activities

EU actions to promote sustainable finance are made up of numerous legislative initiatives (Fig. 3.2.6), which have gradually intensified, particularly after March 2018, when the ***Action Plan on Financing Sustainable Growth***[110] was published. Measures in this area have taken on even greater importance following the launch of the European Green Deal, which announced the revision of the European Strategy on Sustainable Finance. In fact, a distinction has been made between sustainable and unsustainable economic activities. The Commission's expert group[111] published its technical report for a classification system in June 2019. This report emphasises the duty of investors to prove that the investment is oriented towards being sustainable and whether the sustainability criteria have been observed. Together with these publications, guidelines have been defined concerning the measures to be implemented in companies to ensure control over the environmental impact and limit it as much as possible, with reference to the impact of climate change.

The final report on the "EU Taxonomy" of sustainable economic activities[112] was published on 9 March 2020. The document classifies the main economic sectors on the basis of their ability to mitigate or adapt to climate change. These are: those already environmentally sustainable, defined as low carbon; those that pollute, but which cannot be done without and which are asked to do everything possible to shift towards a zero-emission economy but which still cannot be defined as zero carbon, defined as transition; those that are useful to the other two categories which, therefore, allow other activities to have low carbon performance or present a considerable reduction in emissions, defined as enabling. The EU Taxonomy is a robust, science-based tool designed to offer transparency for businesses and investors. The first of the delegated acts of the EU Taxonomy, approved by Commissioners on 21 April, introduces a series of technical screening criteria to define the activities mainly contributing to two of the environmental objectives envisaged by the taxonomy regulation – the adaptation to climate change and climate change mitigation. A second delegated act covering the remaining targets will be published in 2022. Two of the main issues in the EU Taxonomy discussion are the possibility of including investments in natural gas and nuclear power. The decision on these two energy sources, which play a crucial role in the EU (two main sources of the EU electricity generation mix), had been

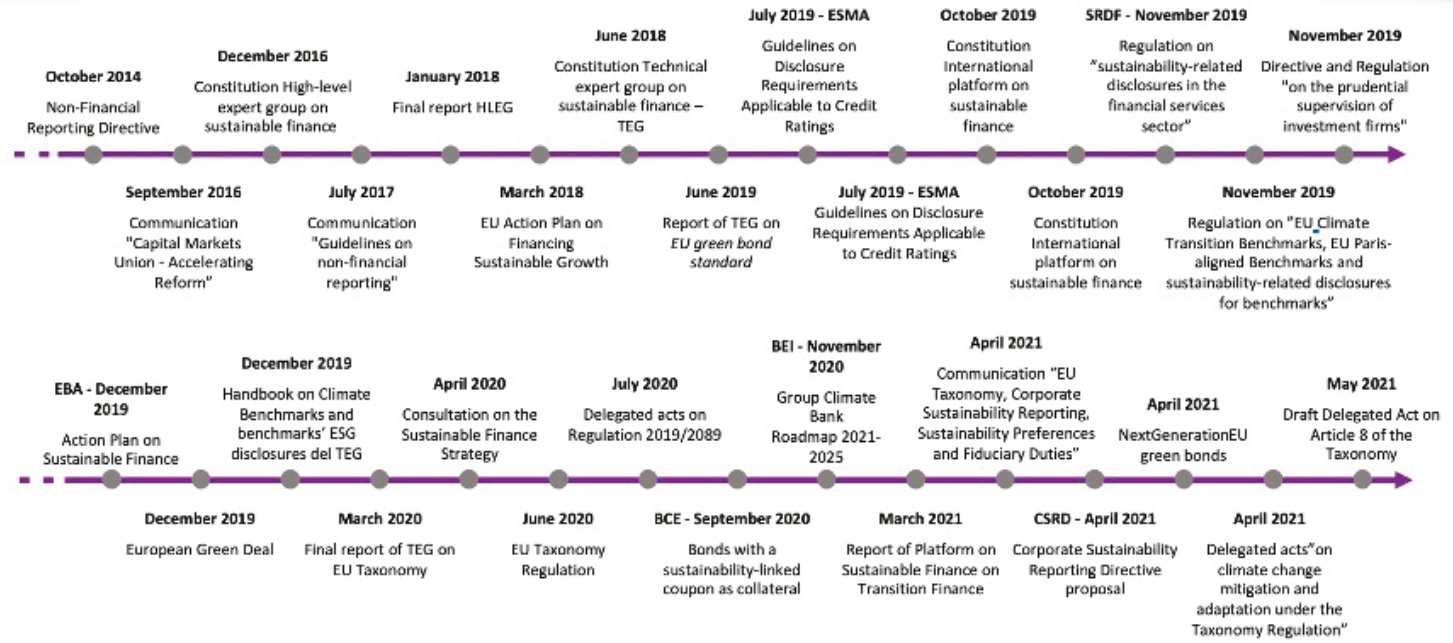
110 Communication from the Commission Action Plan: Financing Sustainable Growth COM/2018/097 final

111 In 2018, the European Commission established a Technical Group of Experts on Sustainable Finance (TEG) to assist it in the development of an EU classification system – the so-called EU Taxonomy – to define: whether an economic activity is environmentally sustainable; a standard for EU Green Bonds; methodologies for EU climate and ESG benchmarks; guidelines to improve corporate disclosure of climate-related information.

112 EU Technical Expert Group on Sustainable Finance, Taxonomy: Final report of the Technical Expert Group on Sustainable Finance, March 2020

Fig. 3.2.6 The main initiatives of the EU institutions for sustainable finance

Source: I-Com elaboration



postponed to the end of the year. In October 2021, the Ministers of Economy and Energy of Bulgaria, Croatia, the Czech Republic, Finland, France, Hungary, Poland, Romania, Slovakia and Slovenia jointly declared that the inclusion of nuclear energy in the European classification is "absolutely necessary", as it is a "reliable resource for a low-carbon future". The role of nuclear power in the energy systems of some countries is indisputable, for example, in France, where 70% of the electricity mix comes from atom energy.

The EU sustainability disclosure obligations will be extended to all large or listed companies, so that nearly 50,000 companies in the EU will have to comply with detailed standards, compared to the 11,000 currently subject to current obligations. The Commission proposes to develop rules for large companies and separate and proportionate rules for SMEs, which unlisted SMEs can use on a voluntary basis. Article 8 of the Taxonomy Regulation requires companies to report how and to what extent their activities qualify as environmentally sustainable, in order to provide investors with uniform and comparable information and prevent greenwashing. Furthermore, non-financial companies will have to disclose the share of turnover and investments linked

to these activities, while financial companies will be obliged to specify to what extent they finance or invest in sustainability. The delegated act under consultation by the Commission provides for different timescales for companies to start reporting. The first disclosure obligations will start from 1 January 2022, while the reporting of the main performance indicators will start from 1 January 2023 (one year later for credit institutions). The EU Regulation 2019/2088 of the European Commission on the sustainability disclosure of financial services (Sustainable Finance Disclosure Regulation, or SFDR) also intervened in the transparency of corporate communications. Entering into force on 10 March, 2021, it strengthens and standardises the reporting requirements of ESG investment processes for financial market participants. Previously, Directive 2019/2034 and EU Regulation 2019/2033 had been published, amending the CRD IV Directive and the CRR Regulation on capital requirements. The directive gives the mandate to the EBA to assess the potential inclusion of environmental, social and governance risks in the review and assessment carried out by the competent authorities, as well as to prepare a report on the introduction of technical criteria for exposure relating to activities that are largely associated with ESG objectives for the supervisory review and evaluation. The regulation mandates the EBA to develop the "technical standards" for the "disclosure" of ESG risks, "physical risks" and "transition risks" by large listed credit institutions and to assess whether a prudential treatment for exposure relating to activities mainly associated with environmental and social objectives, is justified. In April, the Commission also published the proposal for a Directive on "Corporate Sustainability Reporting", which amends the 2014 Directive on Non-Financial Disclosure, strengthening and extending the transparency obligations on ESG matters. Green finance is also an important element of the European exit plan from the Covid-19 crisis. The Commission is aiming to raise 30% of the €750 billion of resources needed to finance Next Generation EU on the markets through the issuance of green bonds. The first issue recorded a demand for more than €135 billion, compared to the 12 billion of securities issued. The high demand allows the EU to place the bonds (with a duration of 15 years) at a lower yield than initially expected, thus saving on interest. Furthermore, all projects and investments financed with the Recovery Fund cannot compromise the achievement of sustainability and environmental protection objectives. Regulation 2021/241, which establishes the Recovery and Resilience instrument, provides for Recovery Fund resources being only used to finance projects that fully respect climate and environmental standards and comply with the principle of not causing any important damages ("Do no significant harm", DNSH), in compliance with Regulation 2020/852. To clarify for MSs how to comply with the DNSH principle in drafting their national plans, the Commission has released a specific technical guide[113] that frames the interpretation of the principle pursuant to art. 17 of the Taxonomy Regulation.

113 European Commission, Commission Notice, Technical guidance on the application of "do no significant harm" under the Recovery and Resilience Facility Regulation, C (2021) 1054 final

An important role in the European context of sustainable finance is played by the European Investment Bank (EIB), which already, in 2007, had launched the first green bond – the Climate Awareness Bond. Since 2012, it has also provided €170 billion in financing for the climate to support projects in Europe and around the world to reduce emissions, and climate mitigation and adaptation for a volume exceeding €600 billion. In more recent years, the EIB has set itself the goal of aligning its actions with the Paris Agreement. To achieve this, it has published a Climate Bank Roadmap, which plans to increase the EIB's funding for climate action and environmental sustainability from around 30% today to at least 50% of the total by 2025, and to support €1 trillion in investments in the same area between 2021 and 2030.

3.3. THE WAY TO A GREENER AND SMARTER MOBILITY

3.3.1. The mobility and transport system in Europe: an overview

The mobility sector is undergoing drastic changes because of the changes in people's behaviour, as well as other external factors. From a social point of view, several recent trends are requiring an adaptation in the mobility sector. These trends are due to the growing number of people moving to (and within) urban areas, the shift towards an even more individual and personalised mobility (due to the growing number of single-person households and the longer life expectancy), and the increase in tourism flows. In the last 50 years, the percentage of the population moving to urban areas has greatly increased worldwide.

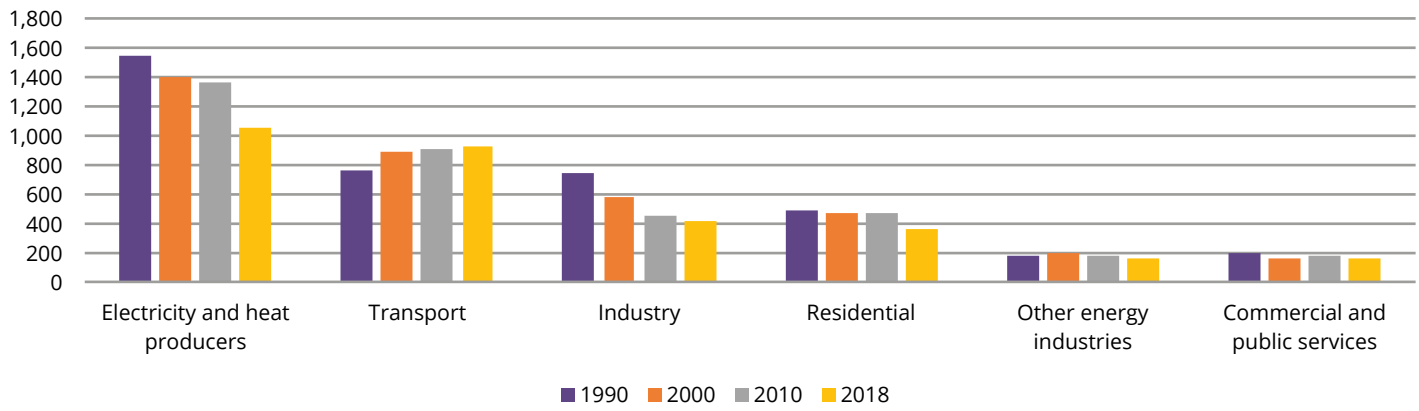
One of the most important challenges facing the transport sector is to reduce the environmental impact. Reducing the pressures of transport on the environment and climate is critical to achieving the long-term vision of EU zero emissions by 2050. Over the last decades, emissions from the EU transport sector have not been dropping enough to limit its environmental and climate impacts. Observing the data published by the IEA relating to EU CO_2 emissions in the period 1990 to 2018 (Fig. 3.3.1), it is clear that, out of the most polluting sectors, only the transport sector has not reduced its emissions. Nowadays, it represents almost a quarter of Europe's greenhouse gas emissions and is the main cause of air pollution in urban areas, posing a health and environmental threat.

Demand for passenger and freight transport in the EU saw a sustained period of growth until 2007-2008. After the peak, in the period 2009-2012, demand for passenger transport remained quite stable with only a slight overall reduction. In contrast, demand for freight transport decreased by up to 11% (between 2008 and 2009) as a result of the economic recession. Since then, demand for passenger and freight transport has been growing. The modal split in passenger transport did not change much in the decade 2010-2019. Passenger cars largely dominated (83%) and accounted for most of the increase in inland passenger transport volumes, followed by aviation. The shares of rail transport and bus and coach services in the passenger modal split remained low (8% and 9%, respectively), not greatly changing between 2005 and 2017 (+1% and -1.4%, respectively). Road freight and waterborne transport (inland waterways and maritime) were responsible for over 85% of total freight transport volumes, followed by rail (11%). During the period 2000-2017, among the other freight transport modes, road freight transport increased the most (24%).

According to the European Environment Agency (EEA), the share of greenhouse gas emissions from the transport mode (2017) sees road transport in first place (71.7%), followed by aviation (13.9%), maritime (13.4%) and rail (0.5%). Although it is important that all transport modes should become more sustainable, it is clear that particular attention must be placed on road transport. The latest version of the ACEA "Vehicles in use, Europe" report (January 2021) highlights how in 2019 the European (UE27) car fleet grew by 1.8% over

Fig. 3.3.1 CO_2 emissions, by sector (EU-28, Mt CO_2)

Source: IEA

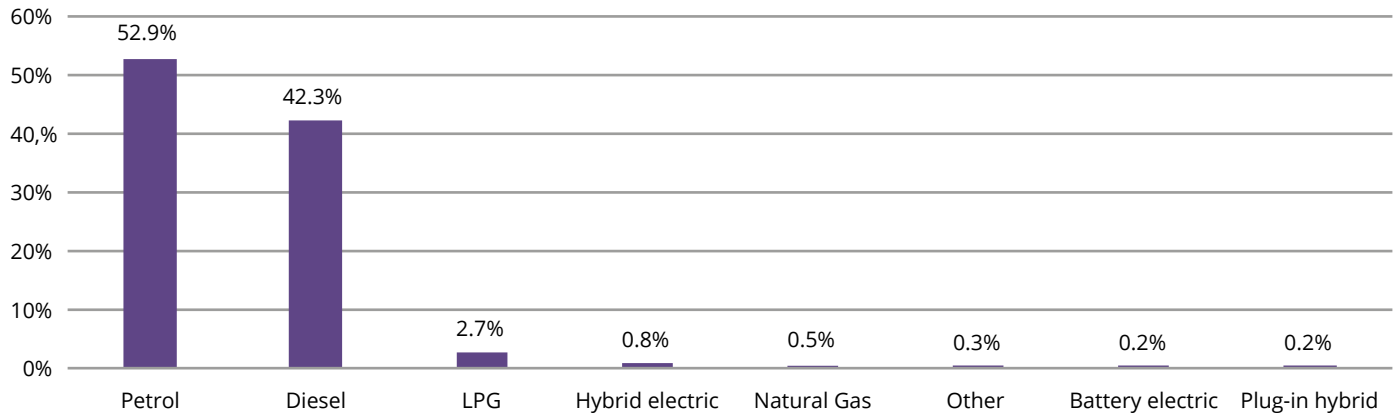


the previous year, reaching 242.7 million vehicles on the road. The highest growth was recorded in Romania (7%), whereas the French car market contracted slightly (-0.3%). The average age of cars on EU-27 roads is 11.5 years, meaning that more than half of the cars currently used by European citizens were purchased before the introduction of the Euro 5 emission standard (January 2011). Lithuania, Estonia and Romania have the oldest fleets, with vehicles older than 16 years. The newer cars can be found, instead, in Luxembourg (6.5 years) and Austria (8.3 years). Despite an increase in registrations in recent years, alternatively-powered cars make up just 4.6% of the total EU car fleet. Only 0.8% of all cars on Europe's roads are hybrid electric, while both battery electric and plug-in hybrids each account for only 0.2% of the total (Fig. 3.3.2). In 2019, almost 60% of all new cars registered in the EU ran on petrol (58.9%, compared to 56.6% in 2018), while diesel accounted for 30.5% of registrations (35.9% in 2018).

As for other types of road vehicles, more than 28 million vans are in circulation throughout the EU. With 6 million vehicles, France has by far the largest van fleet, followed by Italy (4.2 mln), Spain (3.8 mln) and Germany (2.8 mln). Diesel-powered light commercial vehicles make up almost 90% of the EU van fleet, while battery electric vans account for only 0.3%. There are 6.2 million medium and heavy commercial vehicles on the EU's roads. Numbering almost 1.2 million trucks, Poland has the largest fleet, followed closely by Germany (1,010,742) and Italy (946,393). Again, diesel-powered vehicles are the most numerous, with 97.8% of all trucks running on diesel, while petrol fuels 1.3% of the fleet. 0.04%

Fig. 3.3.2 Passenger cars in use, by fuel type (EU-27, 2019)

Source: ACEA



of trucks on the EU roads are zero-emissions. Around 692,207 buses run throughout the EU, with almost half found in three countries alone – Poland, Italy and France. Diesel buses still account for 94.5% of the EU fleet, with only 0.6% being battery electric.

3.3.2. The sustainable and smart mobility strategy

In December 2019, the European Commission released the Communication on the European Green Deal, a strategy aimed at countering the threat of climate change by making the European economy and energy systems technologically sustainable, resource efficient and innovative. The main goal is to achieve, as established by the European Climate Law, climate neutrality by 2050, reducing net greenhouse gas emissions to 0 and achieving full decoupling between economic growth and polluting emissions.

The European Green Deal provides a very dense roadmap of strategic documents and programming plans that include multiple and transversal areas. It includes the need to decarbonise transport, a sector that makes up 5% of the EU's GDP and directly employs about 10 million workers. If the initiative of the Single European Sky, which reduces the fragmentation of European airspace, making the management of the 27,000 flights ordinarily crossing Europe every day more efficient, is expected to reduce emissions by up to 10%, high impact measures need to be taken in order for the Green Deal target to be achieved. For these reasons, the "Sustainable and Smart Mobility Strategy", released by the Commission last December, defines a roadmap of objectives to be achieved in the coming decades.

Specifically, it is expected that by 2030:

- at least 30 million zero-emission vehicles will be on European roads;
- 100 European cities will be climate-neutral;
- high-speed rail traffic will double;
- planned collective journeys of less than 500 km should be carbon neutral within the EU;
- automated mobility will be widespread on a large scale;
- zero-emission ships will be ready for the market.

Instead, by 2035:

- large zero-emission aircraft will be ready for the market.

And finally, by 2050:

- almost all new cars, vans, buses and heavy duty vehicles will be carbon neutral;
- rail freight traffic will double;
- high-speed rail traffic will triple;
- the multimodal trans-European transport network (TEN-T), equipped for sustainable and intelligent transport with high-speed connectivity, will be operational for the global network.

In order to achieve these goals, to reduce transport dependence on fossil fuels and to build a sustainable, smart and resilient mobility system, the Commission envisages the following three pillars of action: 1) make all modes of transport more sustainable; 2) make sustainable alternatives widely available in a multimodal transport system; 3) introduce the right incentives to drive the transition. These three pillars involve measures to significantly reduce current dependence on fossil fuels (e.g., replacing fleets with low and zero-emission vehicles and promoting the use of renewable and low-carbon fuels), tools for orienting activities towards more sustainable transport modes (e.g., increasing the number of passengers traveling by rail and commuters using public transport and active modes of transport and moving a considerable amount of freight on rail, inland waterways and short sea shipping), and the internalisation of external costs by applying the 'polluter pays' and 'user pays' principles through carbon pricing and pricing mechanism tools.

The "Sustainable and Smart Mobility Strategy" is divided into 10 flagships, key areas of intervention, which, in turn, involve 82 actions. Overall, in order to support the sustainable transition of transport, the action plan of the European strategy envisages strengthening the adoption of zero-emissions, renewable fuel and low-carbon vehicles, ships and airplanes and related infrastructures by, for example, installing 3 million public charging points by 2030. It also considers building zero-emission airports and ports and promoting initiatives to foster sustainable aviation and marine fuels. The aim is to make urban and interurban mobility as environmentally friendly as possible, including doubling high-speed rail traffic and considerably developing cycling infrastructure in the next decade. Sustainability measures will also be taken for freight transport, doubling rail freight traffic by 2050. Where tax leveraging is concerned, it is proposed to determine the price of carbon and provide incentives for users, establishing a set of tools to provide fair and efficient prices on all means of transport.

Digitisation will markedly change how passengers and freight move. Here, the goal is to develop connected and

automated multimodal mobility by, for example, allowing passengers to purchase tickets for multimodal travel and goods switching easily from one mode to another. In addition, the Commission wishes to promote innovation and the use of data and AI for mobility, supporting the spread of unmanned aerial vehicles and drones and implementing further actions to build a common European data space on mobility. Finally, the European institutions are considering to make those transport systems strongly hit by the Covid-19 emergency, more resilient. The Single Market will be strengthened by, for example, increasing investments to complete the trans-European transport network (TEN-T) by 2030 and by mobilising both public and private financial resources for the modernisation of fleets in all transport modes. The commitments also include support for mobility safety, also reducing the number of victims to almost zero by 2050. Finally, it is envisaged to make mobility fair for all, promoting passenger accessibility in all regions (including those with reduced mobility), and to make the transport sector more attractive to workers.

3.3.3. Hydrogen and electric batteries to foster the transition

In addition to the Sustainable and Smart Mobility Strategy, the transformation of mobility and transport systems also finds its place in other papers from the European Green Deal – e.g. "A Hydrogen Strategy for a climate neutral Europe" aims to boost clean hydrogen production in Europe. Specifically, it is expected that from 2025 to 2030, hydrogen will become an intrinsic part of our integrated energy system, with at least 40GW of renewable hydrogen electrolysers and the production of up to 10 million tonnes of renewable hydrogen in the EU. From 2030 onwards, hydrogen will be then deployed on a large scale across all hard-to-decarbonise sectors.
Hydrogen can offer alternatives for transport system sectors where it is not easy to reduce emissions, in addition to electrification and other renewable and low-carbon fuels. In the short term, it can be adopted quickly for restricted uses, such as city buses, commercial fleets (e.g., taxis) or certain sections of the railway network that cannot be electrified. Hydrogen filling stations can be easily powered by local electrolysers. At the same time, the use of hydrogen cells in heavy vehicles, including, given the high CO_2 emissions, coaches and special purpose vehicles and for road freight transport over long distances should be encouraged. The 2025 and 2030 targets set out in the CO_2 Emissions Performance Regulation will help create a market for hydrogen-based solutions as soon as fuel cell technology is sufficiently mature and cost-efficient. The IPCEI "Fuel Cells and Hydrogen" funded by Horizon 2020 seeks to accelerate European technological progress in this area.
On commercial rail lines that are difficult to electrify, or where this option is economically inefficient, hydrogen cell trains could be put into operation – currently around 46% of the main network is still run on diesel. Some railway applications of hydrogen cells (e.g., multiple units) can already compete with diesel in terms of cost. Hydrogen could also be a low-emission alternative fuel in short sea shipping and inland waterways, also

considering that the Green Deal also emphasises the need to set a price for CO_2 emissions in this sector.

After 2030, hydrogen and its carbon-neutral CO_2-based synthetic fuels could penetrate a wider range of economic sectors, from shipping to aviation. For longer-range and deep-sea shipping, fuel cell power will need to be increased from one to more megawatts and renewable hydrogen used to produce higher energy density synthetic fuels – methanol or ammonia. In the long term, the possibility of exploiting hydrogen to decarbonise the aviation and maritime transport sector through the production of liquid synthetic kerosene or other synthetic fuels cannot be ruled out. Although these are "drop in" fuels compatible with existing aviation technologies, the implications in terms of energy efficiency still need to be considered. The aviation sector could also include hydrogen jet engines or hydrogen fuel cells, which would require a different aircraft design. In order for these hypotheses to become reality, a roadmap must be defined for the considerable R&D efforts and investments required. In the road transport sector, for example, opening an additional 400 small hydrogen refuelling stations, in addition to today's 100, could require investments of between €850 million and €1 billion[114]. It will also be necessary to act on the demand side so that the use of hydrogen spreads and extends to other applications.

The European Commission is also pushing for the development of electric batteries, key enabling technology for the ecological transition and central to European automotive competitiveness. To this end, in 2017, the Commission had already launched the European Battery Alliance (EBA) in agreement with the EIB, EU countries, industry and the scientific community. The goal is to promote a clean and digital transformation and make Europe a global leader in sustainable battery production and use. Specifically, in line with the European Green Deal, the Circular Economy Action Plan and the Industrial Strategy, the European Battery Alliance plans to develop an innovative, competitive, circular, safe and sustainable battery value chain in the European market, starting from securing access to raw and processed materials, to supporting cell, cell component, battery pack and electric vehicle design and manufacturing and to recycling and disposal in a circular economy.

Recently, the Commission approved a second IPCEI to support research and innovation in the battery value chain prepared jointly by 12 MSs[115] for a total value of €2.9 billion in funding until 2028. This should mobilise €9 billion in private investments, contributing to EU autonomy in the sector. The European institutions expect that by 2025, the actions undertaken under the EBA will help create an industry capable of powering at least six million electric cars each year and producing improvements in performance, safety and environmental impact. 42 companies will benefit from the funding, including SMEs and start-ups, as well as companies active in various sectors such as Tesla, BMW, Fiat Chrysler Automobiles, Enel X, Solvay, Arkema and Borealis.

114 European Commission, Asset study (2020). Hydrogen generation in Europe: Overview of costs and key benefits.

115 Austria, Belgium, Croatia, Finland, France, Germany, Greece, Italy, Poland, Slovakia, Spain and Sweden

The transformation of the transport system also finds its place in the Recovery and Resilience Facility, the extraordinary plan introduced to accelerate European economic recovery. For example, the European Commission encourages MSs to propose flagship investment and reform initiatives aimed at promoting future-proof clean technologies to support the use of sustainable, accessible and smart transport, charging and refuelling stations and extension of public transport. At the same time, the adoption of initiatives to build up the full hydrogen value chain is urged, including renewable hydrogen production, infrastructure (e.g. pipelines), deployment in industry and mobility. While it is true that the EU's hydrogen industries are competitive, they nevertheless require considerable support in order to maintain their technological leadership at this early market phase and grow to create climate neutral solutions and jobs. Similarly, the structuring of the electric battery supply chain is required, starting from the first steps where the EU risks being exposed to dependence on raw material supplier states. Consider, for example, the extraction of primary REE ores and recovery from mining waste, rare earth refining, magnet development, as well as the development of battery-grade lithium refining and of metals and critical raw material capacities.

Transport is also an industry of important proportions, with a significant economic and productive impact and in the EU, it has reached high levels of technology and manufacturing. The pandemic has tested the resilience of the system by disrupting supply chains and, therefore, the lesson to be learnt, involves ensuring they can function even in the most difficult conditions. On the other hand, internalising supply chains would be a factor damaging to the competitiveness of European companies. Consequently, initiatives must be supported to shorten value chains, giving rise to European production chains. Here, the automotive sector is a privileged sector for strengthening European strategic autonomy, starting with the development of integrated supply chains for electric batteries and the nascent hydrogen industry, as well as the Cooperative, Connected and Automated Mobility (CCAM).

CONCLUSIONS

CONCLUSIONS

The twin transition (digital and ecological) and health represent enormous challenges as well as huge opportunities for the future of Europe.

DIGITAL

The European Union is being called on to face enormous challenges arising from digitalisation as it seeks to be a global leader, achieve digital sovereignty and become a model for attracting investment.

The spread of **digital services** has brought obvious benefits to users and has contributed to fostering the development of domestic markets by creating new business opportunities and facilitating international exchanges. Digital services enable a wide range of activities that have become part of everyday life, including the use of marketplaces, social networks, search engines, as well as online brokerage services or applications for a variety of uses (work, games, free time, sharing), which increase the possibilities of consumption, improve the efficiency and competitiveness of the industry and make it easier to participate in civil society.

Digital services are constantly changing, adapting to the context, adding new functionalities and bringing competition to a multidimensional level that tends to develop simultaneously on multiple fronts. The speed with which market trends change is also an element that further complicates the analysis and makes it difficult to produce accurate forecasts on the development of a sector and the possible impact of policy interventions. Furthermore, such a complex context poses demanding challenges for the companies that compete with each other, pushing them to a continuous evolution that leads (for those that have the greatest availability) to investments in the improvement of technologies and services, accelerating and further altering the market dynamics. Sectors such as e-commerce, application stores, social platforms and online advertising are examples of the changing environment in which the different areas of the digital market move.

For these reasons, their design choices and security practices strongly influence user safety online, with the power to shape online content and discussions, as well as digital trade. In the current situation, to stem the spread of unfair practices and harmful content protecting their users, organisations must carry out a careful moderation and monitoring of traffic on their digital platforms.

As regards **online advertising**, even if the protection of privacy is a fundamental aspect to be enforced also in the digital ecosystem, this must not be excessively stringent otherwise it could negatively affect both the quality of the services offered and the growth of the market. Behavioural data allows companies to tailor more specific advertising messages and to choose the most relevant place or moment to convey them. In this way, they help advertisers to better identify the potentially interested user, reducing the percentage of messages delivered to uninterested customer,

so decreasing customer frustration, as well as the marketing campaign costs for the advertisers, and maximising satisfaction. For these reasons, limiting the use of consumer data can be particularly damaging for the advertising industry, without bringing any concrete advantages or further protection for consumers. In 2017, IHS Markit suggested that blocking behavioural advertising would mean a market decrease between 30% and 50% of this segment, which would account for about €8-14 billion in losses per year. Even more importantly, this decrease would affect small players much more (50-70% reduction) than market participants with large-scale first party data (up to a 10% decrease). Where digitalisation is the ground on which the whole world will have to compete, the EU must have a regulatory framework able to encourage innovation, the emergence of new business models and EU competitiveness, as well as providing effective safeguards for users and small and medium-sized enterprises that interact with large platforms.

Online platforms are playing a key role here. Over the last decade, digitalisation has transformed everyday life. Digital platforms especially during the Covid-19 pandemic, have represented the privileged space where individuals can carry out their work, social and leisure activities. The Commission's initiatives to revise the regulatory framework on platforms (DSA and DMA proposals) are necessary and timely but it is important, first of all, to reflect on the ex-ante model proposed to identify the correct balance between the need to ensure legal certainty, on the one hand, and to design a regulatory "future proof" framework, on the other. It is also crucial, in legislative procedures underway, to more thoroughly re-evaluate the type of obligations proposed on suppliers in view of their practicability and sustainability, and in consideration of the impact on security and different business models. Regulatory dialogue as a tool to tailor obligations and sanctions, as based on the most efficient way to pursue a same objective, should be a pillar within the enforcement framework.

Moreover, regulation should offer more choices to consumers and, at the same time, refrain from stifling innovation and, therefore, achieving the opposite (i.e., forbidding or strictly restraining targeted advertising or recommender systems).

Artificial Intelligence deployment is one of the main issues for EU competitiveness.

In the coming years, many segments, if not all, of the economy and daily life will probably be affected by the development of AI technologies and their applications. Therefore, the proposal of an Artificial Intelligence Act is held to be of crucial importance to establishing a solid framework for the protection of European citizens and the development of trustworthy AI technologies.

On the other hand, the EU should take on a leading role in the development of AI technologies and investments, certainly playing a key role in a fast-moving sector. It is of the utmost importance that the EU, MSs and stakeholders act fast to boost the competitiveness of the European AI market. A key element to guarantee the full development of AI in Europe will be a close collaboration between the private and the public

sectors. Moreover, dialogue and exchanges between the EU and national legislations should be further developed before provisions at different levels end up contradicting each other or pursuing different goals. The need to enhance AI development, however, should not prevent the EU from continuing to carefully assess the possible risks of this technology, translating it into the AI regulatory proposal.

Finding the right balance between development of AI technologies and promotion of the model of a trustworthy AI appears to be the only way towards creating a legal framework that will be able to respond to the speed of this fast-growing technology.

AI feeds on **data** so it is essential to continue along the path mapped out by the Commission and to ensure, on the one hand, effective protection of personal data and, on the other, the possibility for businesses and public administrations to have easy access to quality data that can support decision-making processes and make them more effective and efficient.

The development of digital services and technologies is strictly connected with the wide availability of high-performance fixed and mobile **networks**. Europe is working to find its technological autonomy and 5G constitutes one of the pillars on which it is fundamental to base a common strategy. At the same time, Europe seems to have neither the means nor the competences to directly compete with the world leaders. For these reasons, it could be important to strengthen the coordination strategies in terms of frequency allocation, setting up of EU corridors, testbeds and experimentation in new business models, to facilitate the launch of services. However, no single state seems to have sufficient capacity and potential to respond to the pressures of the world superpowers, as would a coordinated action of all the EU countries be able to.

On the regulatory side, the growing complexity and interdependence of an increasing number of different and key stakeholders does not necessarily require more regulation. On the contrary, by supporting investments and development of new services, for the optimal development of 5G, less regulation or more targeted intervention could be more desirable. Indeed, in order to create favourable conditions for investments, the creation of ad hoc policy could be necessary, to support the spread of 5G connectivity and the emergence of new generation services, especially B2B. Therefore, dedicating a large part of resources to expanding optical fibre and upgrading mobile networks to 5G, seems to be a smart move for creating a solid base for developing a new ecosystem. In addition, to reveal the full potential of the European Single Market for the development of new generation services, a further push towards standardisation and interoperability would be desirable.

Although it is important to speed up the development of 5G networks, it is also essential to comply with security standards to guarantee an ecosystem founded on trust.

The digital environment is vast and, therefore, an ideal ground for cyberattacks that can be either indiscriminate or targeted, aimed at large and small

organisations in both the public and private sectors. Therefore, Internet usage and its connected devices offer new opportunities for people and companies but, at the same time, create **new risks**. The range of potential attacks and attackers is wide and becoming more so by the day, up to the point that at the Davos World Economic Forum of 2021 cybersecurity was regarded as one of the greatest economic risks for the ongoing year. The new technologies, mobiles, smart devices connected to the Internet of Things and many AI applications expose both private and public organisations to attackers, increasing the risks of, for example, shutdowns or subversion of industrial control systems. Furthermore, attacks are becoming worryingly more sophisticated and costly to detect. For this reason, the implementation of a common and effective IT security strategy must be one of the main objectives of the EU.

It is also highly important that even companies, and especially large platforms, increase the level of security of their digital systems. According ENISA, the average IT security spending of European organisations is considerably lower than the average for US organisations. The European institutions must, therefore, work to ensure that all the players involved are aware of the extent of the problem, working together to make the IT environment safer.

In order to ensure a secure digital environment, it is necessary to continue along the line outlined by the Commission in the strategy and NIS2 proposal, encouraging the harmonisation of the regulatory framework, increasing investments in skills, re-skills and up-skills and strengthening cooperation mechanisms between states to share and affirm best practices.

HEALTH

The **Covid-19 pandemic** has resulted in a key political lesson – further collaboration is required in Europe to face health challenges. And the EU seems to have learnt the lesson. One way to overcome problems of collective action has been seen in the creation of a public health authority at the European level, with powers beyond the coordination activities carried out by the European Centre for Disease Prevention and Control (HERA). Meanwhile, the EU plan for a stronger **European Health Union** also included a reinforcement of the EMA and of the ECDC. Indeed, the management of pandemics does not respect borders and requires forms of collective action to face the challenges. Moreover, the pandemic has placed a burden on and increased risks for the whole of health management, and demonstrated that investing in health is not a cost but rather a long-term protection for the well-being of citizens and of the entire social and economic context. The EU, not being a "federal" entity, needs to put in place some institutional designs to enforce cross-country collaboration to this end. For this reason, the President of the European Commission, Ursula von der Leyen, in her first speech on the State of the Union, on 16 September 2020, announced the aim to build a Health Union to act with responsibility and unity. Von der Leyen said that the Commission would create a

new European Agency following an idea emerging from the Macron-Merkel summit on May 18, 2020, where it was clearly stated that Europe should regain some sovereignty. It was then taken up in the conclusions of the European Council of 17-21 July.

The **European Health Emergency Preparedness and Response Authority (HERA)** was thus established on 16 September 2021, in order to support the preparation and response capacity to trans-national health emergencies, and to support a European health self-sufficiency programme, especially in the field of pharmaceutical sector dependence on global supply chains. The establishment of a European Biomedical Advanced Research Agency will allow not only for overcoming the fragmentation of the expertise currently scattered amongst various European bodies and organisations, but would also play the role of coordinating the research of diagnostic and therapeutic solutions so as to be prepared for the management of epidemic and pandemic emergencies, unfortunately destined to reoccur over time. In short, the creation of such an agency would implicitly involve the strengthening and increasing of the role of the ECDC whose current mandate is to work with national and EU-level health authorities to facilitate cooperation, and to provide the evidence base needed for effective action.

Meanwhile, the Commission focused on a broader important mission – **reconsidering the European Health ecosystem in the long run**. The pandemic has indeed put an immense strain on European countries, testing the resilience of every country's health and economic systems, together with the ability of the European Commission to develop a coordinated set of responses.

During the very first wave of the pandemic, a number of collaborative EU-level initiatives helped to alleviate supply constraints and support a more coordinated response across countries, and the European institutional response was mainly led by the European Commission. The intervention involved direct financial support for procurement programmes to support healthcare systems, to the support for research in treatments and vaccines, to the medical guidance for MSs, to the coordination of the supply and manufacturing of Personal Protective Equipment (PPE). Amongst the financial responses to rebuild the resilience of the EU macroeconomic system, it should of course be remembered that the EU launched the extraordinary NextGenerationEU (NGEU) programme – the special fund to finance economic recovery in the coming years which includes strengthening EU healthcare systems. In the longer run, the key initiatives to build a European Health Union include a **Pharmaceutical Strategy for Europe**, **crisis preparedness and response measures and the European Plan to Beat Cancer**. Moreover, the recognition of the importance of health data and information in playing a central role to build a strong European Health Union pervades these key initiatives. Therefore, the creation of a **European Health Data Space (EHDS)** still remains one of the main priorities for the Commission, to be developed in a complementary way. Its main objectives are to ensure access and optimal

use of health data, to foster a genuine single market in digital health, and to enhance the development and application of trustworthy digital health products and services. A better access to health data would improve both research and development, and health systems and policies. Data and its use is today a key opportunity for both innovation and policies and the EU-27 data economy is expected to reach €829 billion in 2025. However, the peculiarity of the secondary use of health data (health research and health policy making purposes) requires a specific mechanism and cannot be governed by horizontal legislation alone. Central to this issue is the notion of interoperability, since the exchange of health data to support clinical research and to guarantee new medicines, devices and treatments, will play a key role in the near future. The collection and the storage of data, as well as their interchange between hospitals and among countries, will become increasingly critical for delivering effective healthcare. Here, there is a general consensus on the urge to highlight the quality of data and on its trustworthiness (both raw and processed data).

ENERGY

In the **energy** field, the EU's commitment to a zero environmental impact society is evident from the analysis of the policies undertaken in recent years. Europe is the region of the world that can boast the most marked reduction in **CO_2 emissions** globally in recent decades. In 2020 alone, even considering the pandemic crisis that inevitably affected the emission scenarios, EU CO_2 emissions were 31% lower than in 1990, and 10% lower than the previous year. The EU is also the area with the greatest weight of **renewables** in the energy mix. In 2020, clean energy accounted for a demand share of over 22%, over the EU target of 20%. In the fight against climate change, the Europe cannot exempt itself from assuming the role of the promoter for the transition, and perhaps, above all, regarding the other major world economies. In fact, Europe represents only 8% of greenhouse gas emissions globally, which is a much lower share than North America and Asia. The efforts that European states are making to decarbonise their energy production collide with the decisions of other large economies that continue to focus heavily on fossil fuels. For example, although the Chinese President recently stated that the country will no longer invest in coal-fired power plants outside national borders, further expansion of the use of coal for domestic energy production is foreseen in the five-year plan approved by the Beijing government in early 2021.

Another very important aspect that should not be underestimated concerns the need to carry out a balanced **energy transition**. In recent years, European energy dependence has steadily increased from 56% in 2000, to 58.2% in 2018, up to 60.6% recorded in 2019 (latest data available). With this in mind, though the transition must not expose MSs to the risk of energy poverty, which could trigger a recourse to fossil fuels nullifying the efforts made up to this point. It is also necessary to invest more resources in **research and**

development, especially upon public initiative. In 2020, the European figure on **investments in green technologies** was the lowest in the last ten years, equal to 0.027% of the Union's GDP.

The energy transition will not only have its effects on the energy sector, but will also lead to important changes in the economic structure of our society, affecting many areas, from transport to construction to production and consumption patterns. A transformation of this magnitude, however, requires a global use of **financial resources** estimated by the major international observers between of $4-5 trillion per year. This amount of resources cannot come only from public budgets. On the contrary, the ability to mobilise private investments and to orient the financial and business system in a green direction must be increased.

One of the main points concerns the creation of a shared **taxonomy** on a global level of energy investments, intended as a useful tool to offer transparency to companies and investors. Until now, a sectoral criterion has prevailed to classify an investment as sustainable. However, it is clear that this model does not allow for evaluating the real environmental impact of an investment and favours incorrect practices such as green washing or in any case does not guarantee the achievement of environmental sustainability objectives. Of extreme importance in the financing of the ecological transition is the role of **green bonds**, whose market in the last decade has experienced continuous growth. These tools help bridge the gap between providers of capital and green goods, helping large private companies and governments raise money for projects that aim to achieve climate goals and enabling investors to reach sustainability targets. On the other hand, firm-level surveys show that companies that issue green bonds do not necessarily have lower carbon intensity levels than other companies nor that, after the issue of green bonds, they take on particularly significant trajectories in terms of reducing pollutants. Furthermore, a criticality linked to the use of green bonds is due to the impossibility for small and medium-sized companies to access these forms of financing. Therefore, it is appropriate to provide useful tools to support companies which, due to their size, have difficulty in raising funds directly on the market. To attract capital to green stocks, it is also profitable to provide incentives that allow investors to find such investments attractive. In general, it is necessary that at European level we proceed along the path of defining coherent and common standards, metrics and certifications, as well as with the introduction of disclosure obligations, and that the national institutions accompany the financial and business system on the path of sustainability.

Mobility in Europe must necessarily use this post-pandemic moment to accelerate the sustainable transition. Changes in the transport sector have picked up more slowly than in other sectors. Starting now is essential to meet the European emissions reduction targets for 2030 and 2050. In order to improve the sustainability, security, efficiency, reliability and convenience of transport, a wide set of measures is

required. The decarbonisation of transport and the achievement of environmental objectives is a long process, not achievable in a short time, and requires several hundreds of billions in investments. In this field, the Sustainable and Smart Mobility Strategy provides an important policy direction, as well as the Connecting Europe Facility and Recovery and Resilience Facility, are key EU funding instruments.

However, a **single European transport area** free from barriers and restrictions needs to be created. This is particularly true in the field of railways, which represent a large part of the flows, but it is also valid for air transport, road transport and for all modes. Many European states maintain regulatory constraints that prevent access to foreign operators in the sector, hindering the development of rail transport of passengers and goods within the Union. If the rail market in the EU does not work well, it is not a real alternative to other modes of circulation. On the contrary, it is possible to increase efficiency and reduce transport emissions by breaking down the barriers that divide internal systems and markets within the EU. Freedom of movement of goods and people is also one of the fundamental freedoms of the common European project.

Digitalisation and smart solutions can be an important resource for improving the sustainability and safety of transport. Transport safety is and must also be one of the main objectives of the European institutions in the future, setting the goal of bringing the number of fatalities close to zero. The EU has played a leading role in innovation in the transport sector in recent decades. In order to maintain this leadership, it is important to incentivise investments and research in new digital solutions related to mobility. Digitalisation is a key transformation driver for mobility systems, as well as the spreading of Cooperative Intelligent Transport Systems (C-ITS). Functions with high added value and tasks with a low rate of innovation coexist in the transport and mobility chain. We need to fuel competition to drive innovation while maintaining a high level of ambition.

Another key issue is that of infrastructures both for connection and support for new types of mobility. For instance, the electric charging stations are essential for the increase in **full electric vehicles**, as well as facilities for **hydrogen and alternative fuels**. In this area, we need to accelerate. The risk of not meeting the charging infrastructure targets for electric vehicles is high. Modal switch infrastructures and smart solutions are also very important to encourage the use of public transport and light mobility within urban areas. Furthermore, it would be appropriate to support the spread of measures aimed at making port infrastructures more sustainable and reducing emissions from ships in port, which have a significant environmental impact. The weight of emissions from ships stationed in port on total global emissions was 4% in 2020. It is clear how important it is to work on cold ironing in order to achieve the EU emissions reduction targets. To ensure that this system is successful, however, it is not enough to work only on the

infrastructural side, but also to define rates that make it as convenient as possible for ship-owners. If the use of fossil fuels were in fact less advantageous from an economic point of view than drawing electricity from the quay, then it would be impossible for cold ironing to spread on a large scale. At the same time, it is also important to achieve social objectives and respond to a considerable demand for low-cost transport.

I-Com – Istituto per la Competitività

Rome
Piazza dei Santi Apostoli 66
00187 Rome, Italy
Phone +39 06 4740746

info@i-com.it
www.i-com.it

I-Com – Institute for Competitiveness

Brussels
Square de Meeûs 37
1000 Brussels, Belgium
Phone +32 (0) 27917754

www.i-comEU.eu