icom
institute for competitiveness

I-COM STUDY

THE NEW EUROPE IN THE GLOBAL DIGITAL ERA
Current Rule-Maker, Future Investor?

EDITORS

Silvia Compagnucci

Stefano da Empoli

AUTHORS

Silvia Compagnucci

Maria Rosaria Della Porta

Giusy Massaro

Lorenzo Principali

SUMMARY

1. DIGITAL SINGLE MARKET

1.1. The Digital Single Market within the EU

The Internet and digital technologies are transforming our world. The European Commission has identified that an efficiently functioning Digital Single Market could contribute €415 bln per year to our economy and create hundreds of thousands of new jobs. The Digital Single Market aims to open up digital opportunities for people and businesses and enhance Europe's position as a world leader in the digital economy. Connectivity targets for 2025 have been established to create a Gigabit Society and policies are being pursued to address the barriers and seize the opportunities for digital adoption and development in the EU28 Member States.

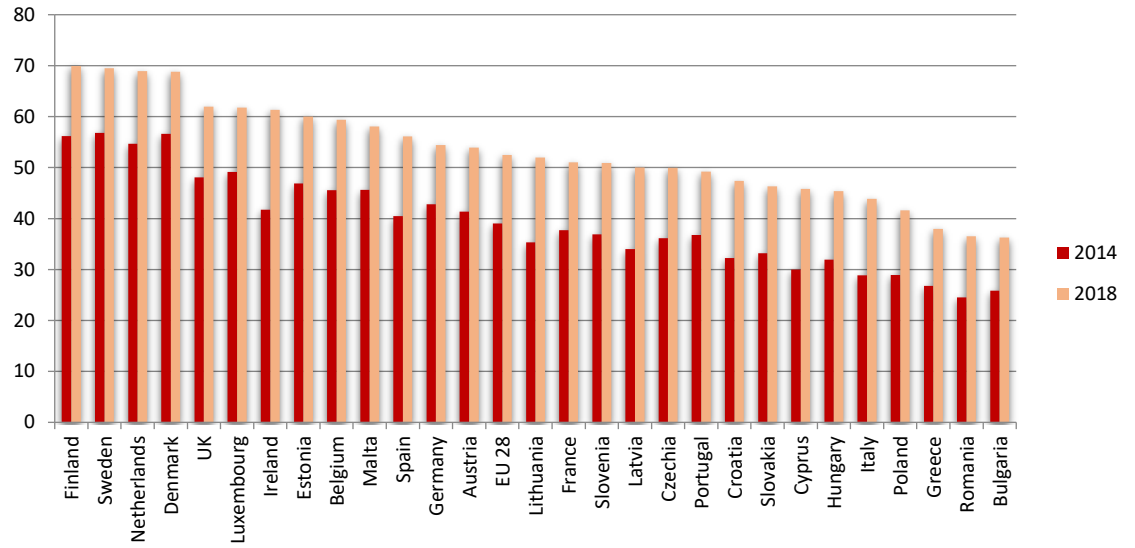
For this reason, it is important to assess the steps undertaken so far by the EU.

The European Commission has developed the Digital Economy and Society Index (DESI), a composite measure that examines Europe's digital performance and helps EU countries identify areas requiring priority investments and actions in order to create a truly Digital Single Market.

For the EU as a whole, in the last five-year period the DESI score has increased by 13.5 points, from 39 to 52.5 (Fig. 1.1). An increase has been registered in all countries, with the northern countries remaining at the forefront of the digital market, and the eastern (Romania and Bulgaria) and Mediterranean (such as Greece and Italy) still lying at the bottom of the ranking. We can see a DESI score ranging from 36.2 for Bulgaria to 69.9 for Finland, a digital divide of 33.7 points, higher than the 32.7 point digital divide registered in 2014.

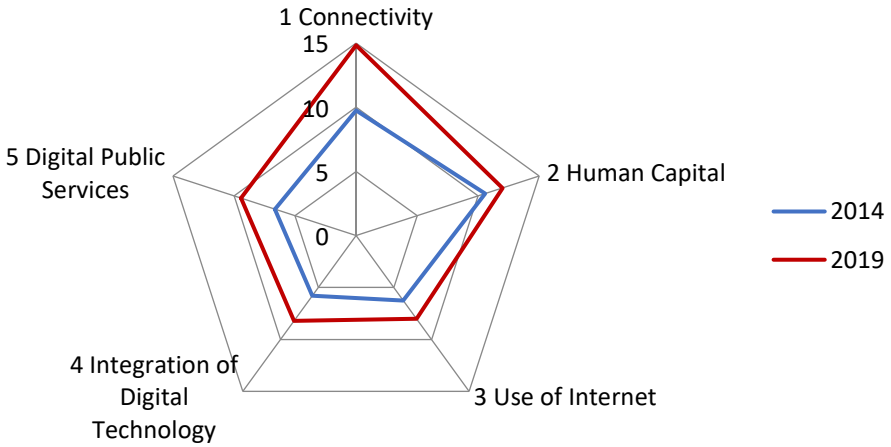
The highest score registered by the EU is in connectivity (14.8) (Fig. 1.2), with the greatest progress occurring (Fig. 1.3) since 2014 (+5 points). This is followed by the integration of human capital (12), although the latter is the least increasing dimension (only 1.4 points in five years).

Fig. 1.1: DESI by Member State



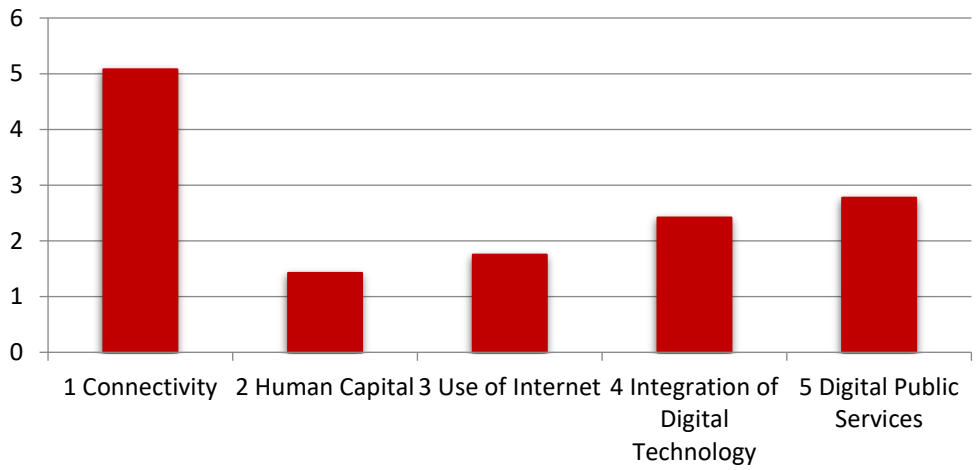
Source: **Digital Scoreboard**

Fig. 1.2: EU DESI by component



Source: **Digital Scoreboard**

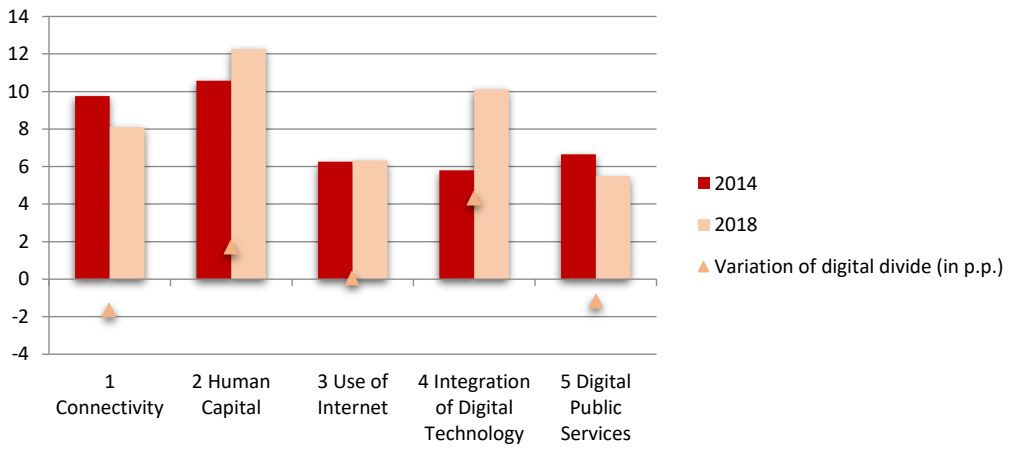
Fig. 1.3: Variation 2014-2018 of EU DESI, by component



Source: I-Com elaboration on Digital Scoreboard data

As already mentioned, the digital divide across EU Member States remains very wide, and only slightly increasing in the 5-year period. This is mainly due to the integration of digital technology (Fig. 1.4) which, though improving greatly, has seen the divide across countries widen. This means that only certain countries – typically, the best performing ones – improved in this respect, while those lagging behind tended to stagnate or struggle to catch up. Connectivity is where the divide shrank the most, followed by Digital Public Services.

Fig. 1.4: EU digital divide by component



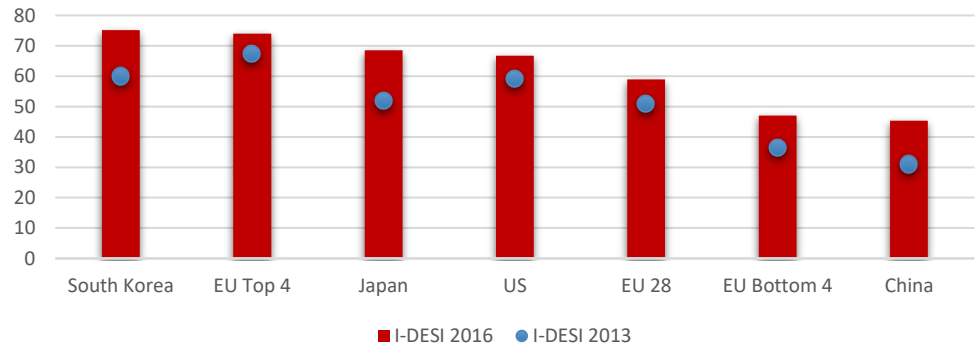
Source: I-Com elaboration on Digital Scoreboard data

1.2. The international context

In order to see a more global perspective, the European Commission drew up the International DESI (I-DESI), a composite measure allowing for comparing the EU with some major world economies (the US, South Korea, Japan and China).

South Korea is the most digitally developed economy (Fig. 1.5), whereas the EU as a whole – with a score of 58.9 – only performs better than China (45.3). Only the best performing EU countries keep up with South Korea, even if the wider gap of 2013 has been narrowed.

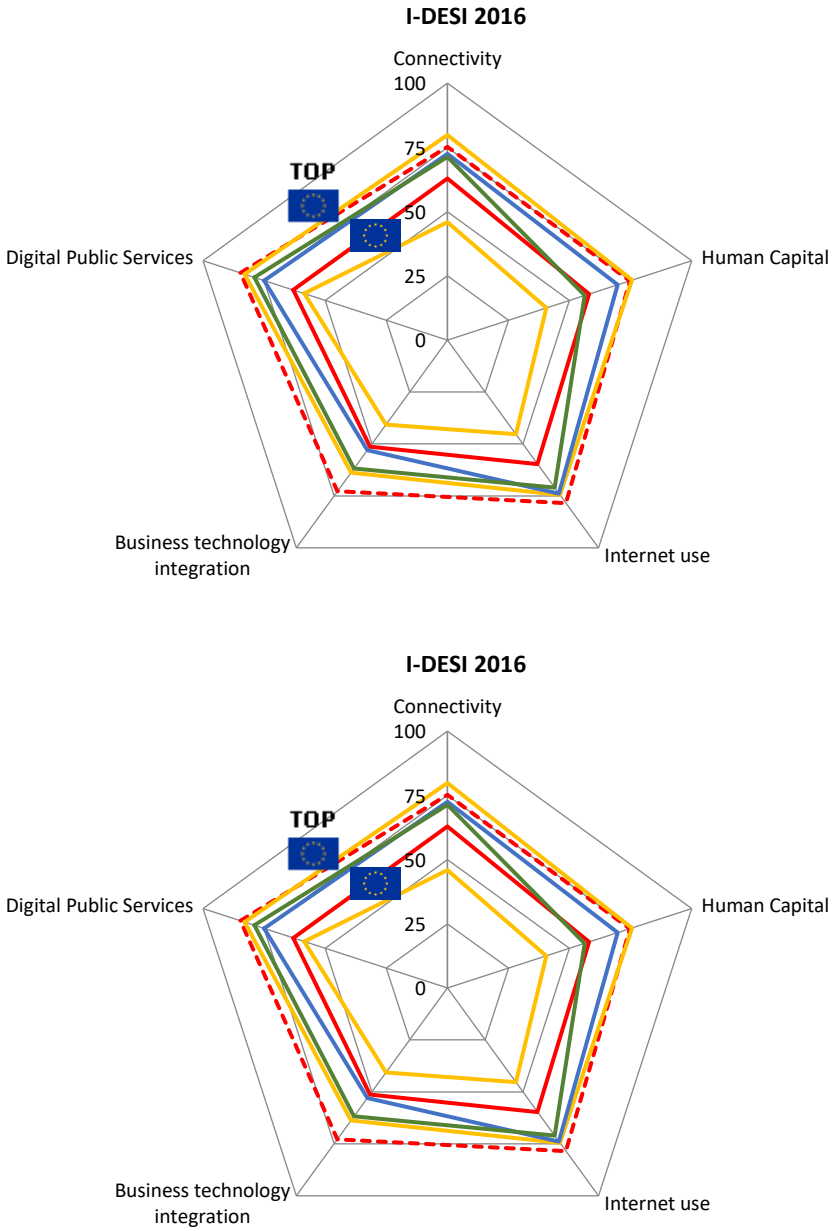
Fig. 1.5: I-DESI



Source: Digital Scoreboard

Looking at the single components of the index (Fig. 6), the EU improved in all in the 3-year period. The largest increase occurred in connectivity (+16.9), followed by Internet usage (+8.7). Less progress was made in digital public services and business technology integration. However, though moving forward, the EU continues to lag behind the major global economies in all of the components. On the contrary, China, way behind in 2013, seems to be catching up quite rapidly.

Fig. 1.6: I-DESI by component (2013 vs. 2016)



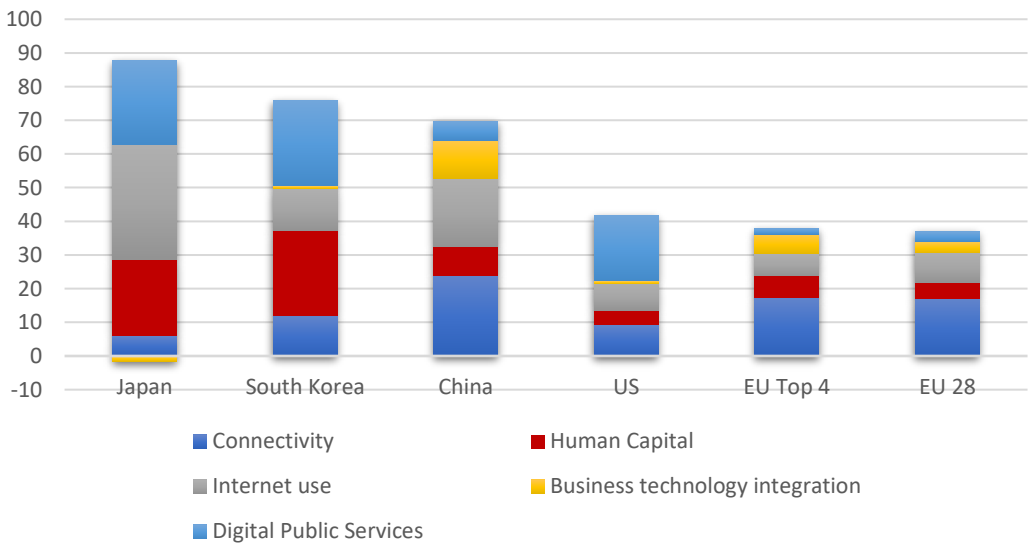
Source: Digital Scoreboard

China is one of the countries with the most important variation over time (Fig. 7). However, Japan and South Korea, already the most developed in 2013, are those registering the most progress,

especially in digital public services and human capital, the components where the EU only made a small improvement.

In general, faster progress can be noted in the Eastern economies. However, the EU is the least improving economy with the top 4 EU countries not performing much better. Yet, it is more or less at the same level as US performance, showing the slow-paced trend of the major Western economies compared to their Eastern counterparts.

Fig. 1.7: Variation in I-DESI score between 2013 and 2016, by country and component



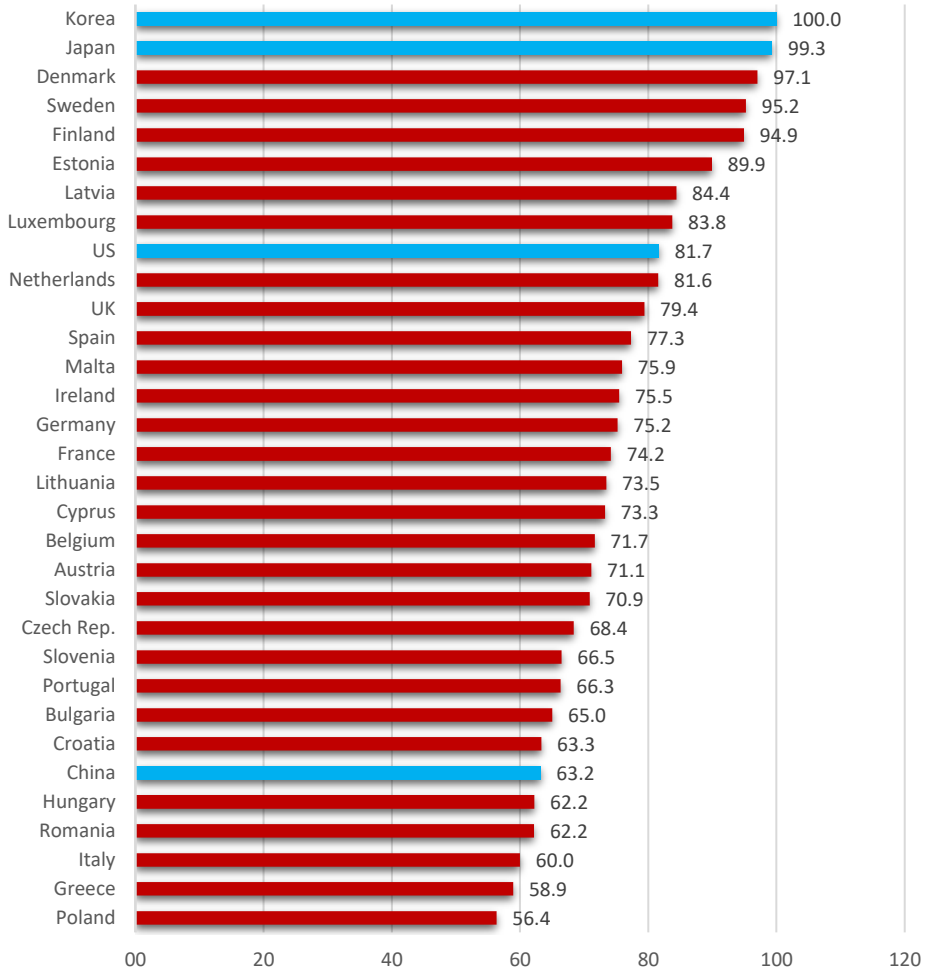
Source: I-Com elaboration on Digital Scoreboard data

In addition, we created an index summarizing the connectivity take-up based on some basic indicators - Internet users, broadband subscriptions (both fixed and mobile) and fiber Internet subscriptions. The index is computed as the mean of the three variables (Fig. 8).

Korea and Japan are ahead, but Northern European countries – Denmark, Sweden and Finland - immediately follow. Denmark stands out for its share of Internet users and fixed broadband subscriptions (97% and 43%, respectively). Where mobile broadband is concerned, Finland is the top country with 154 subscriptions per 100 inhabitants; whereas Sweden performs well for fiber connection take-up (21% of population), being the best European performer, though lagging behind Korea and Japan. Overall, these 3 countries, together with Estonia, Latvia and Luxembourg, do better than the US. On the other hand, China ranks among the lowest positions. Despite the relatively high share of people with a fiber Internet subscription, only slightly more than one in two people in China use the Internet - thus ranking last - and with only 27% of the population subscribed to a fixed broadband contract. In total, China's score is 63.2. At the bottom of the ranking, below

China, we have 5 European countries - Hungary, Romania, Italy, Greece and Poland. Hungary, Romania and Poland especially lag behind in broadband, with Italy and Greece ranking low in Internet usage and fiber connections.

Fig. 1.8: I-Com index on connectivity take-up



Source: I-Com elaboration on World Economic Forum data

1.3.The Digital Single Market Strategy

Considering that the global economy has been rapidly becoming digital and the importance of ensuring that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally, on 6 May 2015, the European Commission launched "***A Digital Single Market Strategy for Europe***" (DSM).

The Digital Single Market Strategy aims to create a market in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence.

It is a very important initiative, having a multi-annual scope and consisting of key interdependent actions - subjected to appropriate consultation and impact assessment - that can only be taken at EU level.

The DSM Strategy is built on three pillars, including **16 specific initiatives**: 1) **better access** for consumers and businesses to online goods and services across Europe; 2) creating the right conditions for **digital networks and services to flourish**; 3) maximizing the **growth potential** of our European Digital Economy.

The first pillar requires the rapid removal of key differences between the online and offline worlds to break down barriers to cross-border online activity, while the second needs high-speed, secure and trustworthy infrastructures and content services, supported by the right regulatory conditions for innovation, investment, fair competition and a level playing field. The third pillar requires investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competitiveness as well as better public services, inclusiveness and skills.

To achieve the objectives of the **first pillar**, the Strategy proposed eight key actions: 1) legislative proposals to simplify and make effective cross-border contractual regulations for consumers and businesses; 2) a review of the Regulation on consumer protection cooperation; 3) affordable high-quality cross-border parcel delivery; 4) preventing unjustified geo-blocking; 5) a survey on competitive practices in the e-commerce sector, relating to the sale of goods or the provision of online services, 6) legislative proposals to reform copyright regulation; 7) revision of Directive 93/83/EC for the coordination of copyright laws and related rights applicable to satellite broadcasting and cable retransmission in order to ensure better cross-border access to broadcaster services in Europe; 8) legislative proposals to reduce the administrative burden arising from the current VAT system and to harmonize the different national systems.

In order to create the right conditions for the development of digital networks and services (**second pillar**), the strategy proposes 5 concrete actions: an ambitious reform of the telecommunications regulatory system, the revision of the Audiovisual Media Services Directive, the analysis of the role

and impact of digital platforms and questions regarding the responsibility of online content, a revision of the E-privacy Directive and the creation of a public-private partnership in the field of information security.

Finally, to encourage European companies to make greater use of technology in the production process (third pillar), the Strategy proposed initiatives on the possession and free circulation of data, the adoption of an integrated plan on ICT standards and the extension of the European framework for the interoperability of public services and an action plan for e-government in 2016-2020.

The following chapters will analyze the most important actions and initiatives adopted by the European Commission within the Digital Single Market Strategy, however, it is important to underline that, since the beginning of the Juncker Commission in 2014, 30 legislative proposals on the Digital Single Market have been made (28 of these have been agreed upon by the co-legislature).

2. DIGITAL NETWORKS

2.1. The spreading of digital infrastructures in Europe

The digital transformation requires increasing network performance, as well the growing data traffic generated by users and enterprises needs a continuous development of data capacity management. Moreover, the spreading of high capacity networks can lead to an increased adoption of cloud computing by SMEs, allowing them to access new generation services such IoT, Big Data and AI. The importance of high capacity digital networks, both wired and wireless, are well known at the European level, since their availability and take-up have enabled the widespread use of products, services and applications in the Digital Single Market. For these reasons, digital networks is one of the topics which has received the widest attention from the European institutions in their legislation and monitoring. For the former, the Commission's strategy on Connectivity for a European Gigabit Society, adopted in September 2016, increased the targets decided by the previous broadband objectives for 2020, which forecasted to supply every European with access to at least 30 Mbps Internet connectivity, and to provide half of European households with connectivity bandwidth of 100 Mbps (see paragraph 2.3). The new targets focus on bringing Internet access with a capacity of at least 100 Mbps to all European households, as well as connecting with performance up to 1 Gigabit the main socio-economics drivers (such as schools, hospitals and other PA entities), covering all urban areas and major land transport routes with a 5G signal.

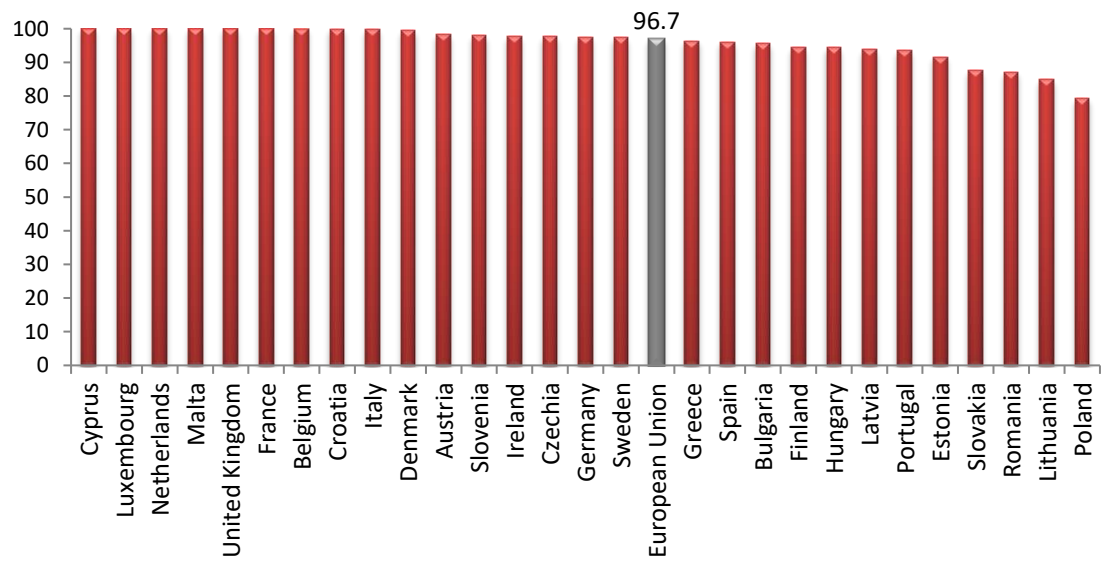
The EU institutions have also set up a funding system which includes the Connecting Europe Broadband Fund, which supports the financing of broadband network infrastructures, and the Connecting Europe Facility (CEF) to foster the deployment and modernization of broadband networks. The latter, which is part of the new EU 2021-2027 budget, should, with € 3 bln in funds, finance strategic digital connectivity infrastructures. It will be decided by the end of 2019.

Concerning the monitoring of the progress in digital network availability, starting in 2014, the European Commission published the Digital Economy and Society Index (DESI), a composite index updated every year which measures progress of EU countries towards a digital economy and society[1].

Broadband connection is widely available all over Europe, as shown in Fig. 2.1. On average, broadband coverage reached 96% of European households, while the only countries registering less than 90% of household coverage, though above 80%, are Slovakia, Romania, and Lithuania. Poland is the only country below the latter threshold.

[1] The DESI Index does not focus on digital networks only, but is made up of approximately 30 indicators related to Europe's digital performance and tracks the evolution of EU Member States, across five main components - Connectivity, Human Capital, Use of Internet, Integration of Digital Technology, Digital Public Services.

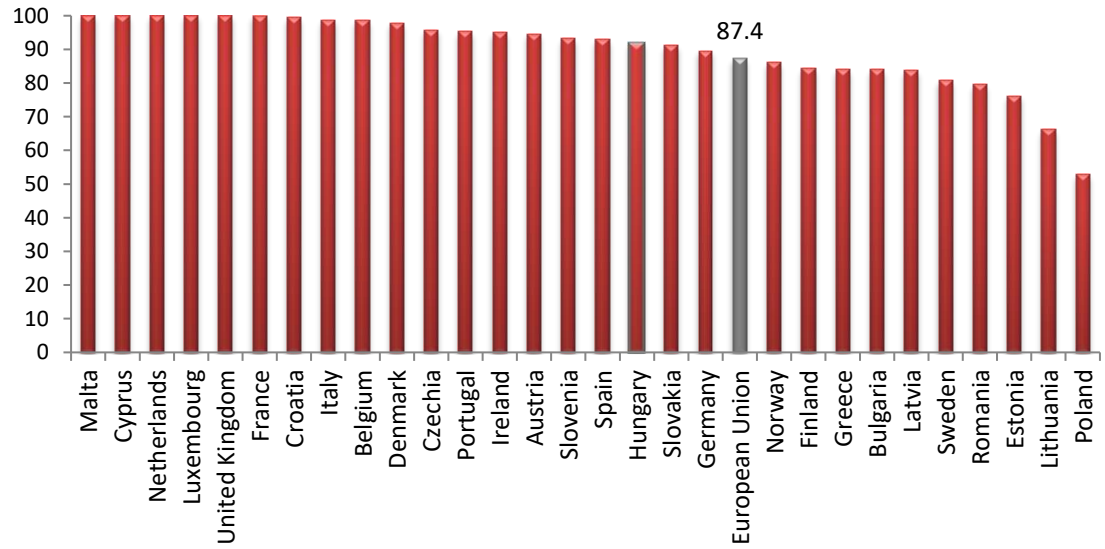
Fig. 2.1: Standard fixed broadband coverage/availability (% of households)



Source: European Commission, Digital Scoreboard

Broadband coverage of rural areas reached 87.4% of households in 2018 (Fig.2.2). This classification, also revealing the lower dissemination in highly digitalized countries such as Norway, Sweden and Estonia, shows how these values are linked to the morphology of the different national areas.

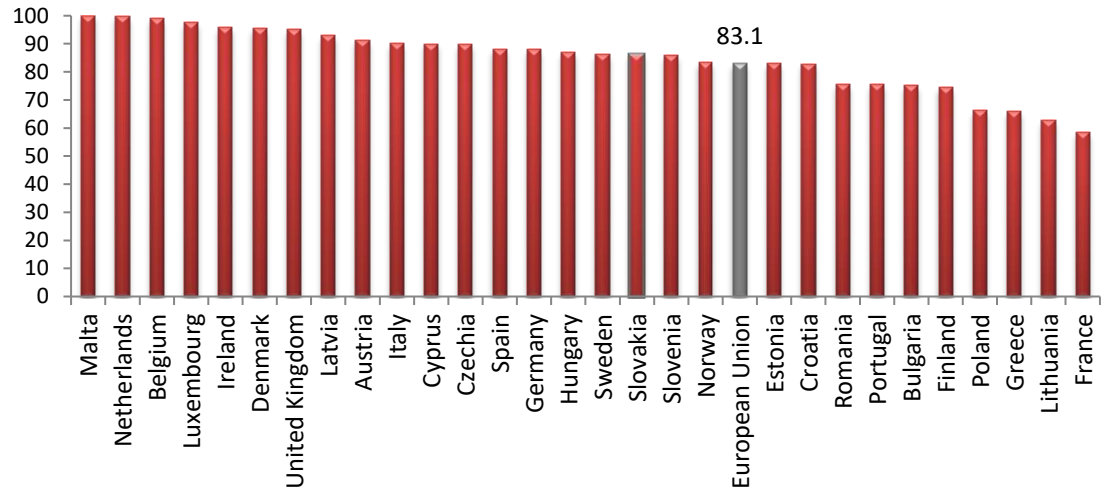
Fig. 2.2: Rural standard fixed broadband coverage (% of households, 2018)



Note: Rural areas are defined as those with less than 100 people per km^2.
Source: European Commission, Digital Scoreboard

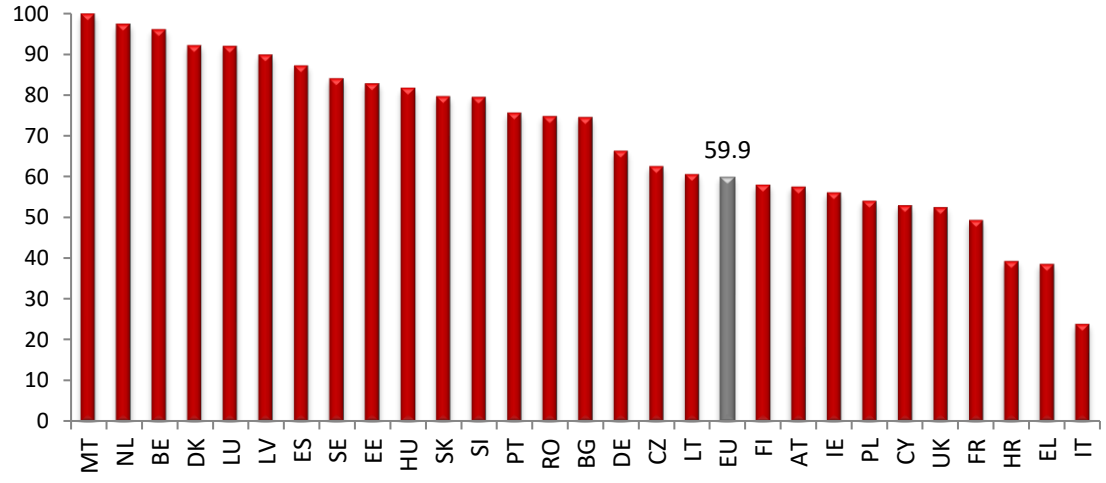
Looking at the progress made by EU countries in providing connections capable of a download speed of at least 30 Mbps to all of their households, the threshold reached a 83.1% peak in 2018. On the one hand, the spread of connectivity around Europe appears to have achieved a very good result. On the other hand, it will be hard for EU countries to reach the full coverage by 2020, as established by the European Digital Agenda's previous targets.

Fig. 2.3: NGA broadband coverage/availability (% of households, 2018)



Note: Fast broadband is a connection with download speeds of at least 30 Mbps.
Source: European Commission, Digital Scoreboard

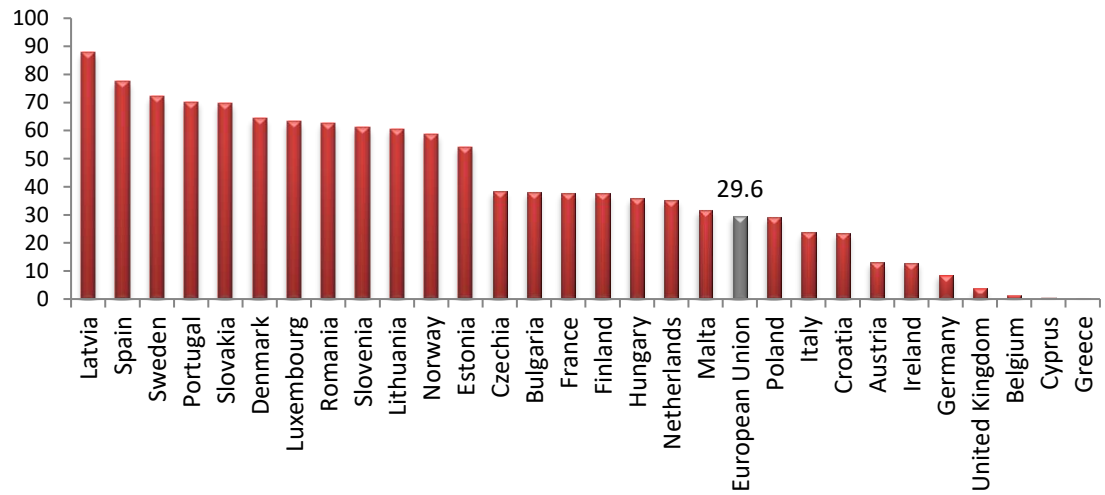
Fig. 2.4: Ultrafast broadband coverage (% of households)



Note: Percentage of households covered by broadband of at least 100 Mbps download. Considered technologies are FTTH, FTTB and Cable Docsis 3.0
Source: European Commission, Digital Scoreboard

For ultrafast networks, the threshold reached by EU infrastructures related to this parameter is in line with the objectives set in 2010 for the second pillar of the European Digital Agenda. At least 50% of the population is covered by ultra-fast broadband Internet services above 100 Mbps. In 2019, almost 60% of European households have been covered by ultrafast digital networks, including fiber to the home (FTTH), fiber to the building (FTTB) and cable connectivity (Cable Docsis 3.0).

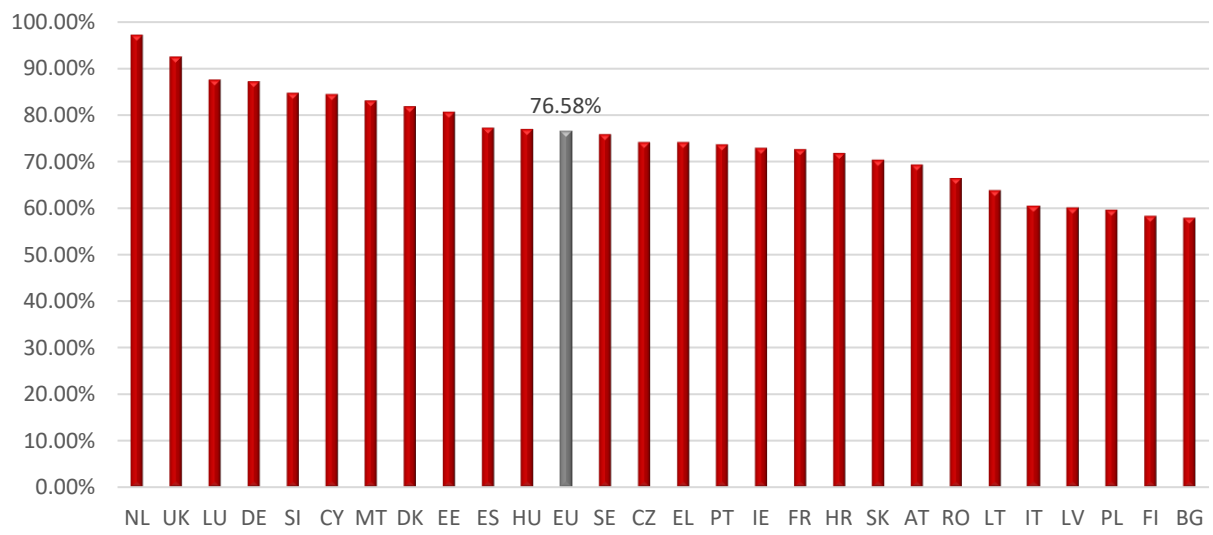
Fig. 2.5: Fiber to the premises coverage/availability (% of households, 2018)



Note: Coverage is a supply indicator defined as the percentage of households living in areas served by FTTP
Source: Broadband coverage in Europe, studies for the EC by Point Topic (2011-2012 figures, SMART 2011/0027 and 2012/0035) and IHS and Valdani, Vicari & Associati (2013 figures, SMART 2013/0054) in European Commission, Digital Scoreboard

Another interesting indicator is related to the availability of optical fiber, that shows the capability of providing Internet connection of up to 1 Gbps. Fig. 2.5 shows the coverage percentage of households living in areas served by FTTP, that reached almost 30% in 2018. Differently from 100 Mbps speed, which can be achieved through different technologies, the up-to-1Gbps connections require the spread of optical fiber to the premises (buildings or homes). Almost half of the EU countries reveal excellent performance, with more than 50% of households connected. On the other hand, many other countries, such Austria, Germany and the United Kingdom, which can count on digital cable connectivity, reveal a lower fiber distribution, being a disadvantage in the long term and in reaching the goals connected to the achieving the Gigabit Society.

Fig. 2.6: Households with fixed broadband connections (%)



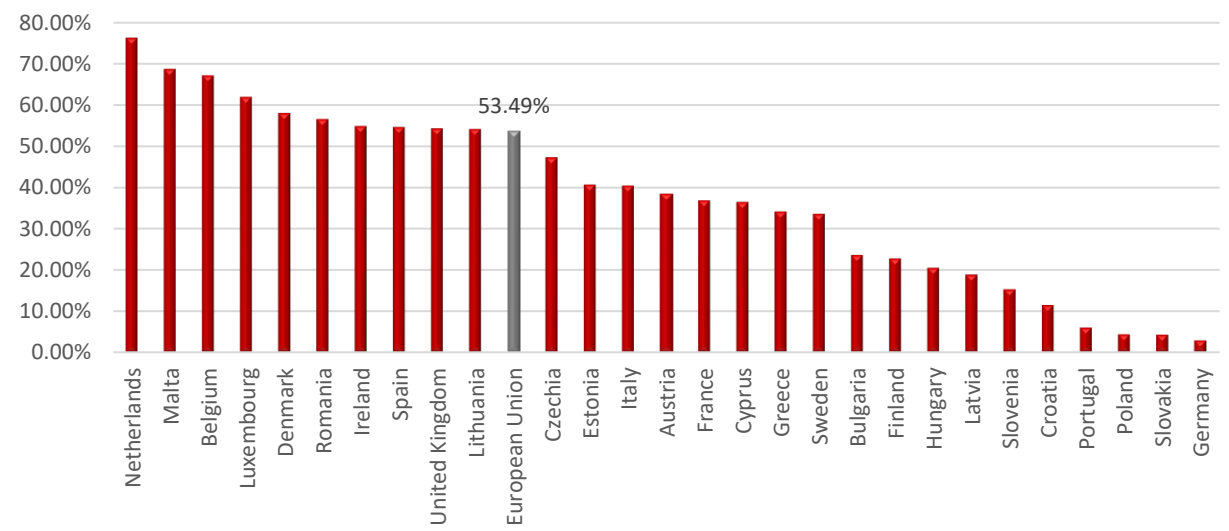
Source: European Commission, Digital Scoreboard

If the availability and coverage of households appear extremely important, another fundamental indicator is related to the effective take up of the Internet access service. Currently, 75% of European households have adopted a broadband connection service (Fig. 2.6). Only three countries show figures lower than 60%.

At the same time, the adoption of fast broadband services reached almost 55% of European households (Fig. 2.7). Northern countries appear to have the highest adoption percentage (especially the Netherlands, Malta, Belgium and Luxembourg), as well as Romania and Spain, while those with the lowest rates are Portugal, Poland Slovakia and Germany.

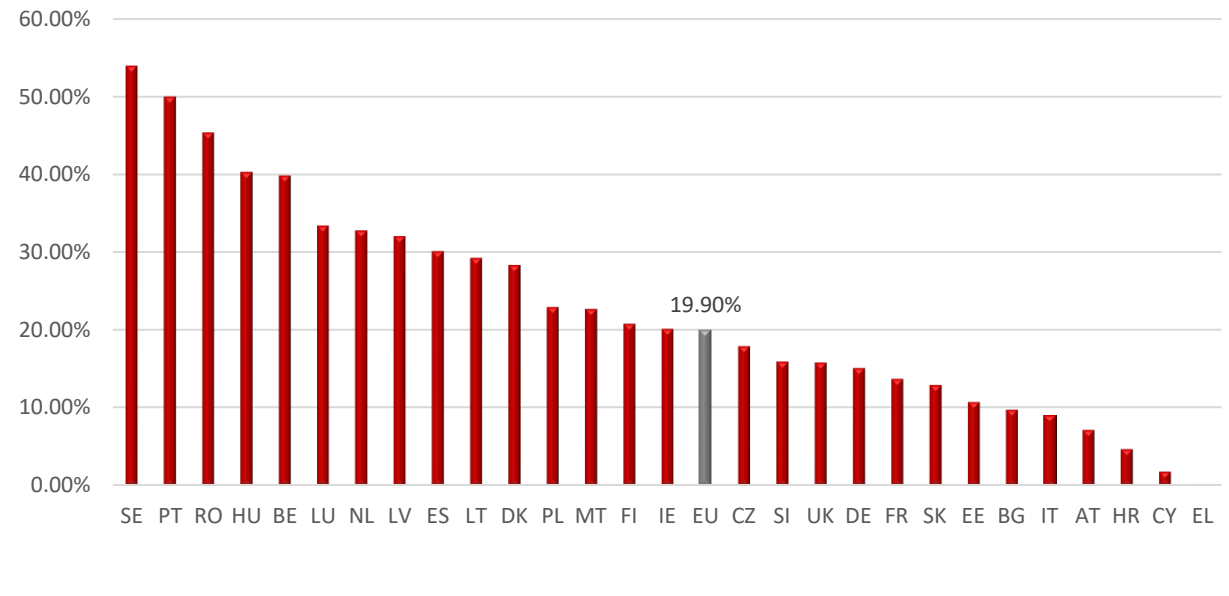
For at least 100 Mbps connection adoption, considering the target of 50% of EU households, the current average is actually below 20%. Only 2 countries reached the 50% adoption threshold, while 5 countries do not even reach 10% (Fig. 2.8).

Fig. 2.7: Fast Broadband take-up (% of households, 2019)



Note: Percentage of households subscribing to broadband of at least 30 Mbps
Source: European Commission, Digital Scoreboard

Fig. 2.8: Households with an ultrafast broadband subscription (% of households, 2018)

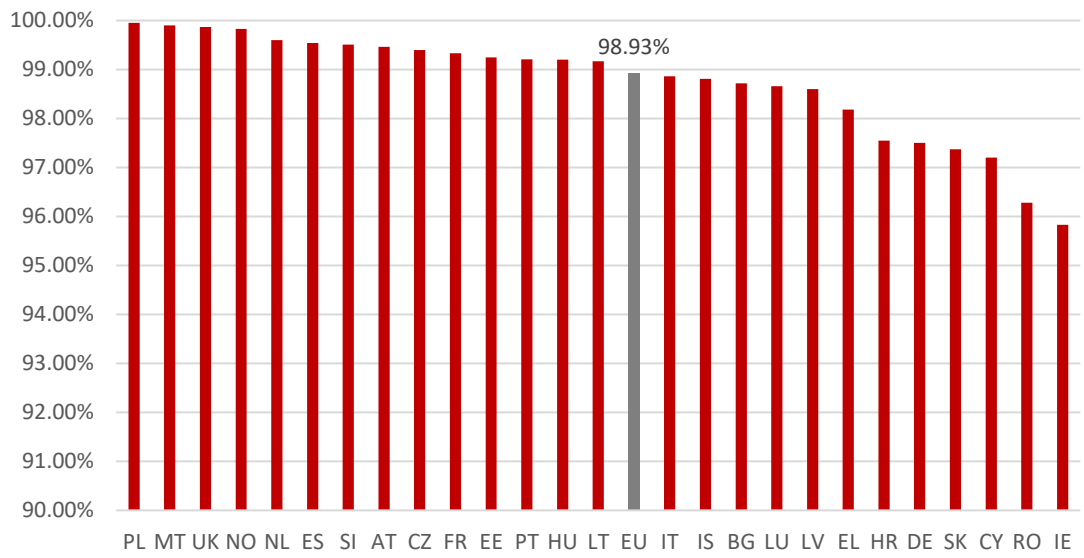


Note: Households with a broadband connection of at least 100 Mbps
Source: European Commission, Digital Scoreboard

2.2. Mobile connections and the road to 5G

If fast and ultrafast wired broadband system is currently developing, the mobile broadband infrastructure with high download capacity is already widely available. According to the data provided by the operators and the EU Commission, the mobile networks supply 4G (LTE) broadband capacity to almost 99% of European households. Moreover, even in the three countries with the lowest levels (Cyprus, Romania and Ireland), the coverage is well above 95% (Fig. 2.9).

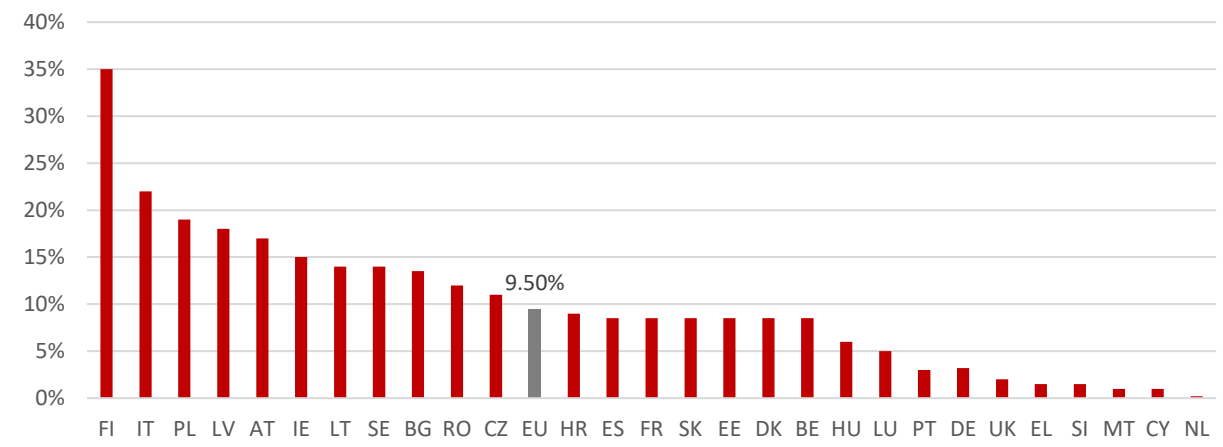
Fig. 2.9: 4G mobile broadband (LTE) coverage (% of households)



Source: European Commission, Digital Scoreboard

Mobile networks have become such good performers that about 10% of European households only use mobile to connect to the Internet. This is especially so in Finland and Italy. The reasons why households prefer to adopt mobile broadband rather than fixed depends on a mix of reasons that include wired connection availability and competitive subscription prices provided by mobile carriers.

Fig. 2.10: Households using only mobile broadband at home (% of households), 2018



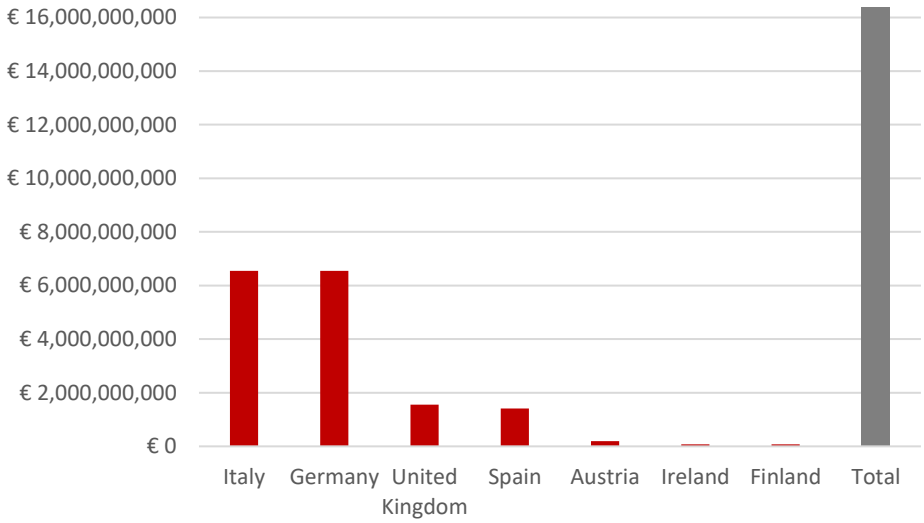
Source: Eurostat

For these reasons, as well as for the contribution it can provide for the spread of the Internet of things and, as well, the economic benefits resulting from its technical features, it is extremely important for the EU institutions to speed up the upgrading to 5G networks and the construction of new infrastructures supporting the new mobile standard.

Regarding the economic advantages, the study commissioned by the European Commission to a consortium made up of Trinity College, Tech4i2, Real Wireless and InterDigital (2016) found that 5G could produce benefits of up to € 113 bln per year in 2025, coming from automotive (€ 42 bln), transport (€ 8 bln), smart workplaces (€ 30 bln), smart cities (€ 8 bln) and suburban areas (€ 10 bln). While benefits are consistent, the same can also be said for the investments required to implement the new 5G technical environment. First of all, in countries such as Italy and Germany, the spectrum auction price overtook the € 6 bln threshold. Currently, the amount spent in Europe is above €16 bln, and there are still many more spectrums to assign, as well, many countries, such as France, still have to launch their national auctions (Fig. 2.11).

Comparing the pioneer band for 5G (3.4-3.8 GHz), the price per MHz paid in Italy is by far the most expensive, taking into account the license length and number of inhabitants (Fig. 2.12).

Fig. 2.11: Auction results for 5G frequencies in Europe (2018-2019)



Source: I-Com elaborations on various sources, 2019

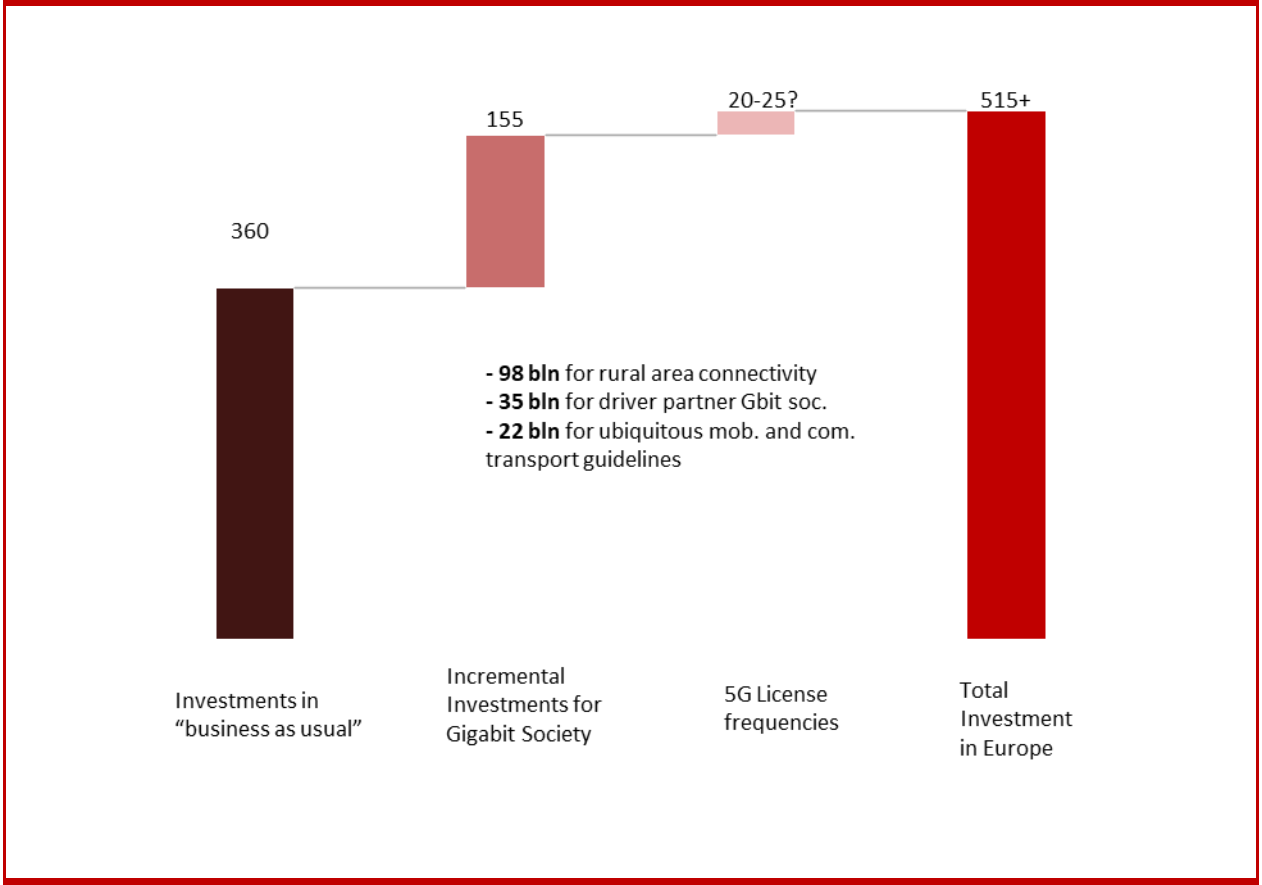
Fig. 2.12: Costs of 5G Frequencies: International Comparison

Countries	Price x MHz (in €, per 1000 ab.)	Expenditure	Length (years)	Population (2018)	Width (MHz)	Band
Italy	€ 19,98	4.346.820.000 €	18	60.431.280	200	3.6-3.8 GHz
Germy	€ 8,39	4.175.529.000 €	20	82.927.920	300	3.4-3.7 GHz
Spain	€ 7,55	1.410.700.000 €	20	46.723.750	200	3.6-3.8 GHz
United Kingdom	€ 5,73	1.143.714.909 €	20	66.488.990	150	3.4-3.6 GHz
Austria	€ 5,59	188.000.000 €	20	8.847.040	190	3.4-3.8 GHz
Ireland	€ 2,98	78.000.000 €	15	4.853.510	360	3.6-3.8 GHz
Finland	€ 2,56	77.000.000 €	14	5.518.050	390	3.4-3.8 GHz
Latvia	€ 2,42	7.000.000 €	10	1.926.540	150	3.4-3.8 GHz
Czech Rep.	€ 1,87	39.673.387 €	10	10.625.690	200	3.6-3.8 GHz
Hungary	€ 0,16	2.760.000 €	20	9.768.780	90	3.4-3.8 GHz

Source: I-Com elaborations (2019)

Generally speaking, investments required for the implementation of the 5G networks have been estimated as more than €515 bln, coming from the so-called "business as usual" segments (about €360 bln) as well as from the incremental investment for the Gigabit Society (€98 bln for rural area connectivity), while €35 bln are required for socio-economic driver connectivity and €22 bln for ubiquitous mobility and connection of transport routes.

Fig. 2.13: Estimated necessary investments for the implementation of the 5G network in Europe (€ bln, 2017-2025)

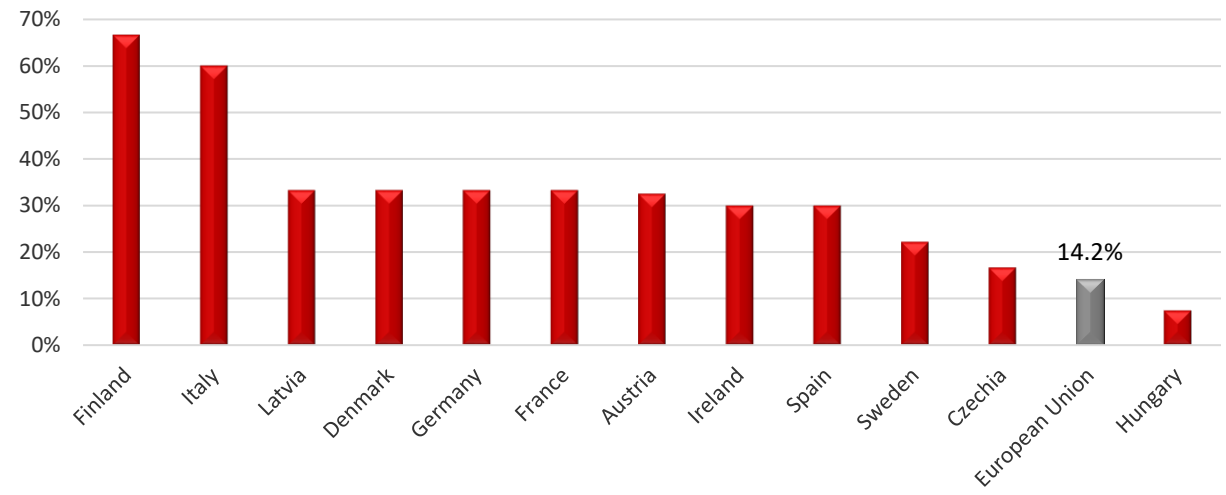


Source: European Commission Connectivity for a Competitive Digital Single Market (2016)

Fig. 2.13 shows how spectrum allocation is very far from being complete, with less than 15% having been auctioned by September 2019, while there are only 2 countries (Finland and Italy) which have allocated more than half of the dedicated bands. At the same time, 6 countries are conducting a wider number of 5G experiments, showing that the interest of both national bodies and private operators for the new mobile transmission standard is high. Overall, considering the possible economic and social benefits, the operators' investment efforts, as well as the race of foreign

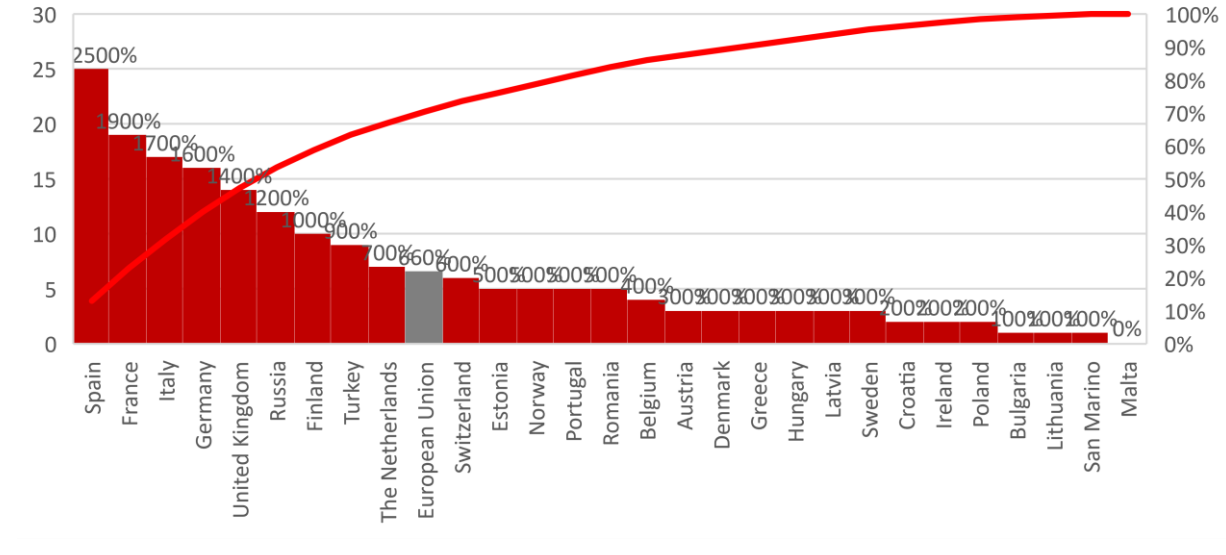
countries such as South Korea and the economic super powers, China and the US, to implement the new standards, a start to study incentives that could accelerate the spread of 5G within Europe could be a sensible measure.

Fig. 2.14: 5G Readiness in European Countries



Source: 5G Observatory (2019)

Fig. 2.15: 5G trials by country



Source: 5G Observatory

2.3. The European Regulatory Framework

The availability of advanced telecommunication networks and technologies is a precondition for digital services development and usage by individuals and companies.

To ensure that everyone in the EU will have the best possible Internet connection to participate in the digital society and economy, on 14 September 2016, the Commission launched a connectivity package with a set of measures to encourage investment in very high-capacity networks and accelerate the roll-out of 5G wireless technology and free Wi-Fi access points in public spaces. These measures included the European Electronic Communications Code and the revised BEREC Regulation, common broadband targets for the Gigabit Society, a plan to foster European leadership in 5G technology and a support scheme for public authorities to offer free Wi-Fi access to their citizens.

In December 2018, the European Electronic Communications Code was approved and entered into force. It is an important initiative to simplify and modernize the regulatory framework, provide incentives for fiber investments for wholesale only operators and incentives for co-investment in fiber networks and introduces new opportunities for national regulators to access civil and core infrastructure elements and longer market review periods for ex-ante regulatory decisions (5 years instead of 3) to provide greater certainty to operators.

The Code has introduced a series of important innovations including the scope of application of the regulatory framework, access regulation, radio spectrum management, universal service and consumer protection. On the scope of application, the Code has provided a new definition of an electronic communication service capable of including over the top (OTT), although with different intensities depending on the usage (or not) of numbering resources for OTT communication services.

As for the regulation of access, the Code has strengthened national regulatory authorities' powers introducing the possibility to impose symmetrical access obligations (towards all operators) in the presence of not repeatable network elements. In such cases, the Code allows for the imposition of access to wiring and related resources within buildings or up to the first point of concentration or distribution if located outside the building.

With regard, instead, to the asymmetric regulation (for operators with significant market power - SPM), the traditional system remains unchanged, even if the Code has enhanced the principle according to which the obligations relating to the access must be proportionate, they must pursue the objective of facing situations of actual failure of the market and must be prescribed only if necessary for the protection of the end user's interest. Within this framework, the same Code has introduced a new procedure for the identification of transactional markets entrusted to the competence of BEREC - whose powers and competences, in general, have been strengthened in

the Code - and has set in 5 years (instead of 3) the deadline for the renewal of market analyses. A significant change is seen in the reduction of the regulatory burden, in the presence of certain conditions, for operators with SPM, in case of co-investments to set up new high-capacity networks for co-investment, as well as for operators "wholesale only". In view of the advent of 5G and the roadmap set by the European Commission since 2016, the new Code contains provisions aimed at accelerating and coordinating the procedures for assigning radio spectrum for electronic communications services and networks. The new rules also pursue a goal of harmonization with respect to some key issues of licensing models and authorizing regimes, including the minimum duration of individual user rights licenses (at least 15 years), encourage the resolution of critical issues related to interferences (national or cross-border) and, in a logic of efficiency, highlights the importance to support the shared use, transfer and rental of the spectrum based on the principle "use it or lose it".

The Code has also updated and redefined the scope of universal service obligations (eliminating outdated services, such as public pay telephones) and has encouraged Member States to ensure their citizens have access, at affordable prices, to an adequate broadband Internet access service and voice communication services. Finally, as for consumer protection, the Code has set new transparency obligations in relation to conditions, prices and quality of electronic communication services, given end users the right to have free access to at least one comparison tool of the various services offered, introduced provisions aimed at simplifying the transition from one operator to another, avoiding lock-in effects, such as the rules on the maximum duration (two years) and the termination of contracts, the scope also being extended to service packages.

If the Code has strengthened the powers and the role of BEREC, Regulation (EU) 2018/1971 completes the provisions of the Code simplifying the governance structure and the decision-making processes of this body.

With regard to connectivity goals, the Commission launched a strategy on Connectivity for a European Gigabit Society, setting a vision of Europe where availability and take-up of very high capacity networks enables the widespread use of products, services and applications in the Digital Single Market. The strategy has confirmed the previous broadband objectives for 2020 (that are to supply every European with access to at least 30 Mbps connectivity and to provide half of European households with connectivity rates of 100 Mbps), but has also fixed 3 main strategic objectives for 2025: 1) Gigabit connectivity for all of the main socio-economic drivers; 2) uninterrupted 5G coverage for all urban areas and major terrestrial transport paths: 3) access to connectivity offering at least 100 Mbps for all European households.

To achieve these ambitious objectives, the Commission launched other initiatives. In particular, the Communication "*5G for Europe: an Action Plan*" (published in September 2016 together with the working document "5G Global Developments") has identified 8 actions to encourage 5G

development: 1) promoting preliminary trials from 2017 onwards and pre-commercial trials with a clear cross-border dimension from 2018, encouraging the adoption by Member States of national 5G deployment roadmaps and the identification of at least one major city to be "5G enabled" by the end of 2020; 2) identifying, according with Member States, by the end of 2016 a list of pioneer spectrum bands for the initial launch of 5G services; 3) adopting an agreement on the full set of spectrum bands (below and above 6GHz) to be harmonized for deployment of commercial 5G networks in Europe; 4) setting roll-out and quality objectives for the monitoring of key fiber progress and cell deployment scenarios identifying best practices to facilitate – also incrementing administrative conditions – denser cell deployment; 5) promoting by the end of 2019 the availability of the initial global 5G standard, the standardization on radio access and core network challenges and the conclusion of cross-industry partnerships; 6)planning technological experiments to be carried out as early as 2017 and presenting detailed roadmaps by March 2017 for the implementation of advanced pre-commercial trials; 7) encouraging Member States to consider 5G infrastructure's usage to improve the performance of communication services used for public safety and security; 8) identifying assumptions and modalities for a venture financing facility. They were mainly focused on asking Member States to identify 5G pioneer frequencies, adopting national roadmaps, promoting trials, making a global standard available and identifying a city to achieve full 5G by 2020.

Considering the importance and the impact of 5G networks and the critical issues on security, on 26 March 2019, the European Commission recommended a set of operational steps and measures to ensure a **high level of cybersecurity of 5G networks** across the EU. Specifically, the Recommendation sets out a series of operational measures, encouraging Member States to conclude a national risk assessment of 5G network infrastructures by the end of June 2019. It underlined that EU Member States exclude companies from their markets for national security reasons, if they do not comply with the country's standards and legal framework, supporting exchange of information and the activity of the Commission and the European Agency for Cybersecurity (ENISA). It also included completing a coordinated risk assessment by 1 October 2019.

In this context, the **Connecting Europe Broadband Fund (CEBF)** contributes to the achievement of the European Gigabit Society objectives. It aims to raise €500 mln for broadband investment by 2020 and is expected to unlock total investments of €1-1.7 bln.

The deployment of telecommunications networks is also supported by the **Connecting Europe Facility (CEF)**. It promotes trans-European networks and infrastructures in the sectors of transport, telecommunications and energy allocating to Telecom, in the current programming period, a budget of approximately € 1 bln, € 870 mln being earmarked for Digital Service Infrastructures (DSIs) delivering networked cross-border services for citizens, businesses and public

administrations (the rest is for connectivity networks). For the 2021-2027 period, the Commission proposed a budget of € 3 bln, mostly for connectivity, but still subject to an agreement on the overall long-term EU budget.

Other resources have been allocated to network deployment by Horizon Europe and the Multiannual Financial Framework for 2021-2027.

To encourage digital inclusion, the Commission also launched the WiFi4EU initiative which promotes free access to Wi-Fi connectivity for citizens in public spaces including parks, squares, public buildings, libraries, health centers and museums in municipalities throughout Europe. It has allocated € 120 mln to provide all interested local authorities with the possibility to offer free Wi-Fi connections to their citizens. The WiFi4EU initiative provides municipalities with the opportunity to apply for vouchers to the value € 15,000 that are to be used to install Wi-Fi equipment in public spaces within municipalities still not equipped with a free Wi-Fi hotspot.

3. DATA DRIVEN INNOVATION IN EUROPE

3.1. The data and Big Data market

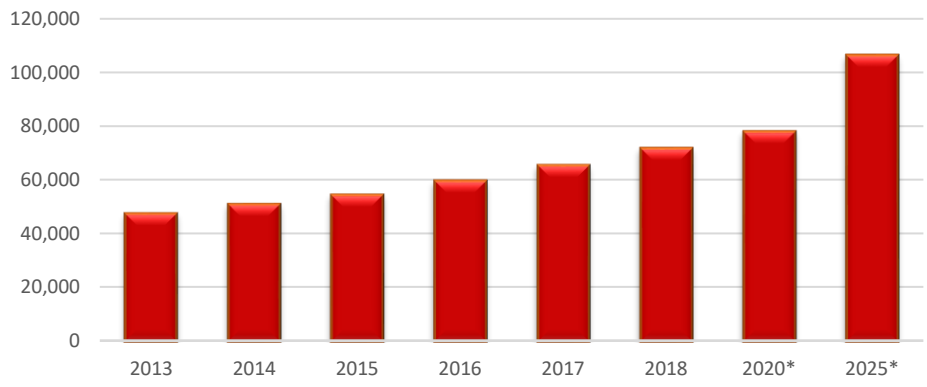
Data-driven innovation stands out as a key pillar in the 21st century sources of growth. The confluence of several trends, including the increasing migration of socio-economic activities to the Internet and the decline in the cost of data collection, storage and processing is leading to the generation and use of huge volumes of data.

According to the OECD, in 2017, the global data traffic per month reached 120 exabytes (billion gigabytes), about 70 times the traffic existing in 2005.

Mobile phones continue to be the largest category of connected devices. However, in 2018, they were expected to be surpassed by IoT devices, which include connected cars, machines, utility meters, remote metering and consumer electronics[2].

The data market value – meant as the aggregate value of the demand for digital data without measuring the direct, indirect and induced impacts of data on the economy as a whole – is expected to increase from the current € 71.6 bln to approximately € 78 bln in 2020 and € 106 bln in 2025 (Fig. 3.1), with the UK, Germany, France and Italy accounting for 64.6% of the total. Sweden is the highest-growth country, registering a compound annual growth rate between 2016 and 2020 of 14.1%, more than twice the EU average (5.8%) (Fig. 3.2).

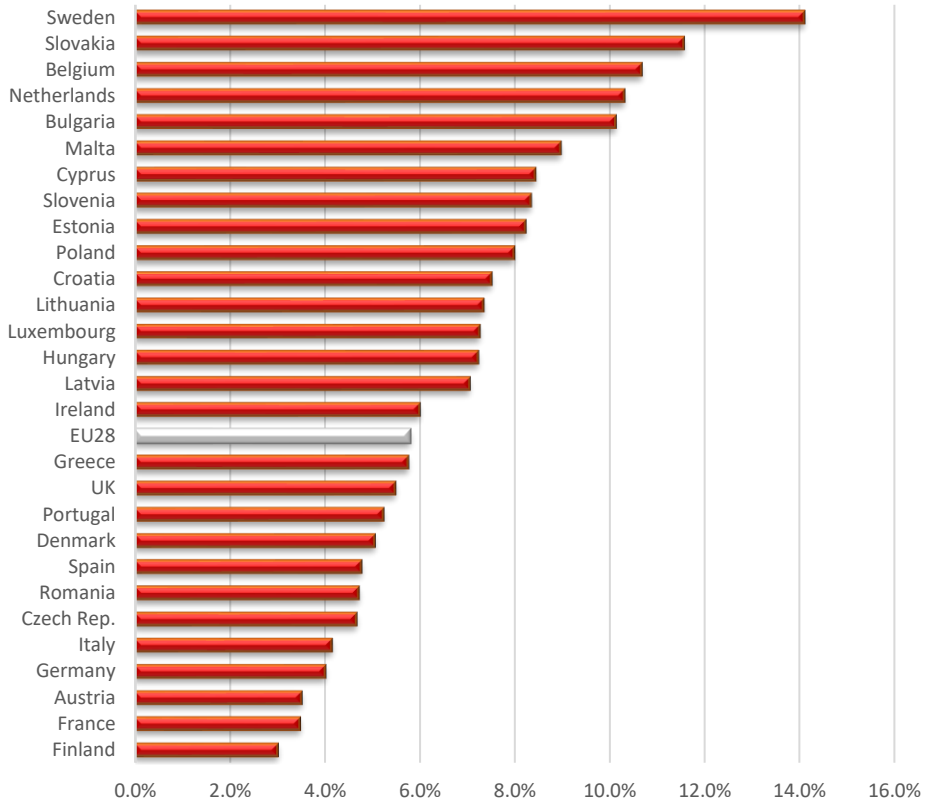
Fig. 3.1: Data market value



Source: I-Com elaboration on data European Data Market Monitoring Tool, IDC (2019)
* Estimate

[2] Ericsson (2016).

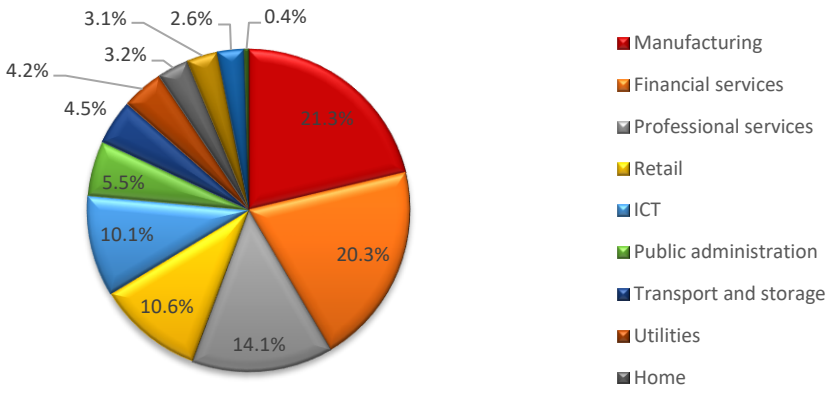
Fig. 3.2: Compound annual growth rate (CAGR 2018-2025*, by country)



Source: I-Com elaboration on European Data Market Monitoring Tool, IDC (2019)
* Baseline scenario

Manufacturing and financial services lead in terms of data market size, with a value of € 15 bln and € 14.5 bln, respectively (Fig. 3.3). Surprisingly, ICT is ranked only 5th, although, by definition, it is one of the sectors registering the highest use of data-related technologies. However, after professional services, ICT is the most dynamic vertical market (7% and 6.4%, respectively, of yearly growth rate in the 2018-2025 period for the two sectors). Less dynamic, are the construction and public administration sectors (with an approximately 4% yearly growth).

Fig. 3.3: Data Market Value by Industry (2016)



Source: I-Com elaboration on European Data Market Monitoring Tool, IDC (2019)

Big Data is a specific subset of data that refers to the changing, large and disparate volumes of data being created by people, tools and machines. Recent technological breakthroughs have exponentially reduced the cost of data storage and computing, making the storage of more data easier and less expensive than ever before. With an increased volume of Big Data now cheaper and more accessible, more accurate and precise business decisions can be made. Data sets have become so voluminous that traditional data processing software is unable to manage them. However, these massive volumes of data can be used to address business problems which in the past would never have been able to be tackled.

New, innovative and scalable technology is now required to collect, host and analytically process the vast amounts of data gathered to derive real-time business insights that relate to consumers, risk, profit, performance, productivity management and enhanced shareholder value.

Platforms are at the centers of the Big Data ecosystem (Fig. 3.4), being the main interface between consumers and other market players. Working besides them, we find:

1) Content providers (journals, websites and application developers), which create the informative content displayed by both search engines and other platforms such as social networks;

2) Sellers or service providers, which offer products and services to the final consumer in exchange for money. This category includes manufacturers, wholesalers, professionals, real estate agencies, consultants, finance institutions and any other types of businesses that may use platform marketing channels to persuade consumers to purchase their products;

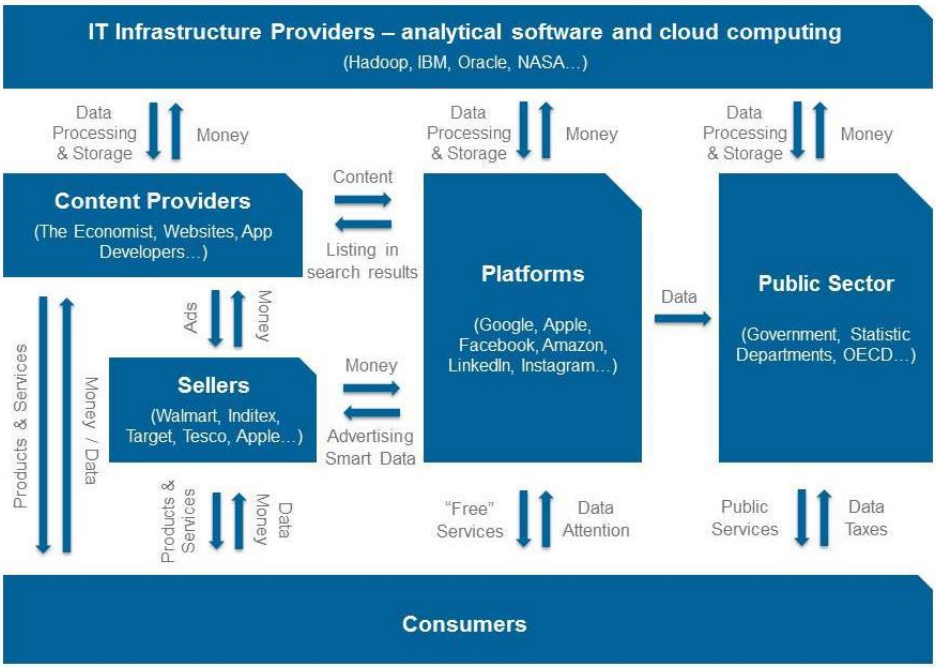
3) IT infrastructure providers, which develop the relevant software to handle Big Data, but, most importantly, provide cloud computing and storage. That is, they act as third-party data centers where companies can store and process their data on-demand;

4) The public sector (central and local governments, public hospitals, clinics, social security and other public services), that collects Big Data from citizens, thus becoming one of the most data-intensive sectors of the economy.

According to Big Data market forecasts, its value should grow markedly by 2026 (on average, +13% per year) (Fig. 3.5), mainly driven by the software segment.

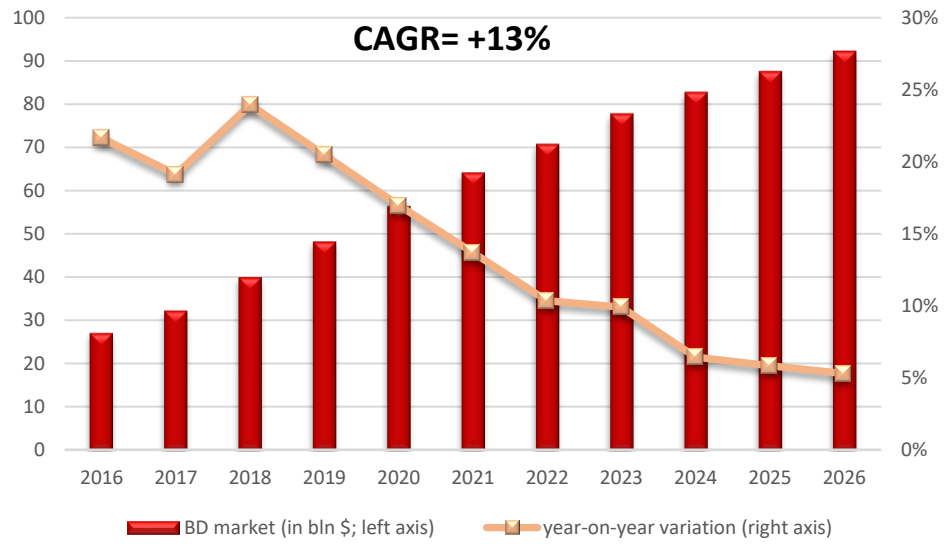
Even if the growth rate gradually declines, within a decade, it will have risen from $ 27 to 92 bln.

Fig. 3.4: The Big Data ecosystem



Source: OECD, 2016

Fig. 3.5: The Big Data market



Source: I-Com elaboration on Wikibon Big Data Project (2016)

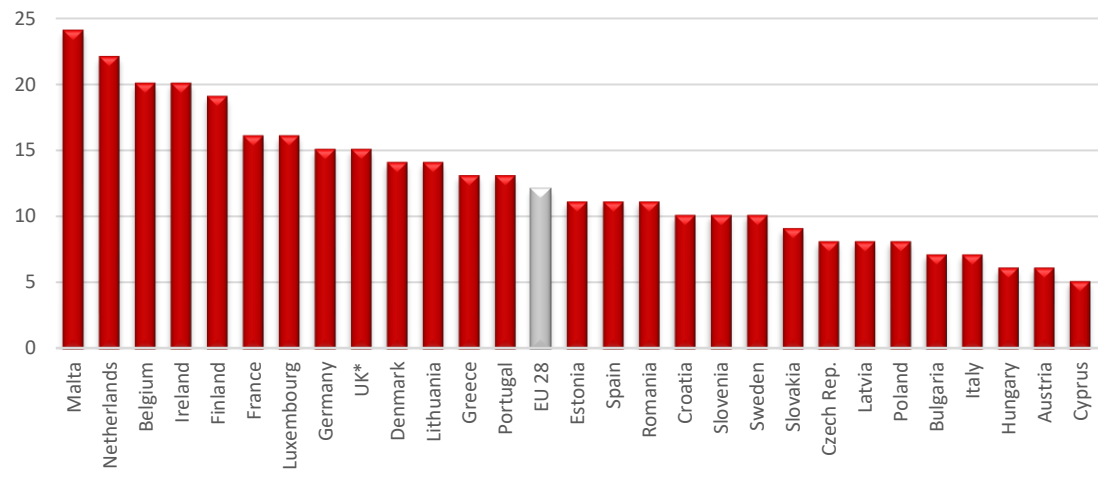
Being able to harness Big Data can lead to important and positive gains for a business, which, in turn, may benefit consumers, employees and society as a whole. The use of Big Data for innovative and creative purposes, in a process known as data-driven innovation (DDI), allows companies to improve the quality of their products and develop entirely new services. As well, using Big Data is also convenient for businesses to generally improve their production efficiency, forecast market trends, improve decision-making and enhance consumer segmentation. Although the efficiency gains from data driven-innovation are inherently hard to measure, some studies suggest that DDI users benefit, on average, from a 5% to 10% faster productivity growth than similar companies not using DDI[3]. In addition to the overall productivity gains, the use of Big Data can lead to other important social benefits that are usually not accounted for in standard measures. These benefits concern, among others:

- the transport sector, by reducing traffic congestion, through the tracking of mobile devices, and then providing time and fuel savings;
- the electricity sector, by reducing the cost of CO2 emissions, through the adoption of smart grid applications;
- the healthcare system, where, through the creation of electronic health records, it is possible to reduce medical errors, improve diagnosis and increase efficiency in management and pricing.

[3] OECD, "Data-Driven Innovation: Big Data for Growth and Well-Being", 2015

Nevertheless, despite the undeniable benefits of Big Data, the implementation of the so-called Big Data Analytics (BDA) is still low. Eurostat data shows that only 12% of European companies make use of BDA tools (Fig. 3.6). The best performing countries are Malta and the Netherlands where, however, less than one company in four uses such tools.

Fig. 3.6: Enterprises performing big data analysis (2018)



Source: I-Com elaboration on Eurostat data

3.2. Data-driven innovation and its impact on the economy

Slightly different from the data market value is the concept of data economy. The data economy measures the overall impacts of the data market on the economy as a whole, involving the generation, collection, storage, processing, distribution, analysis elaboration, delivery and exploitation of data enabled by digital technologies. The data economy also includes the direct, indirect and induced effects of the data market on the economy. Thus, it aggregates direct, indirect and induced impacts of the data market.

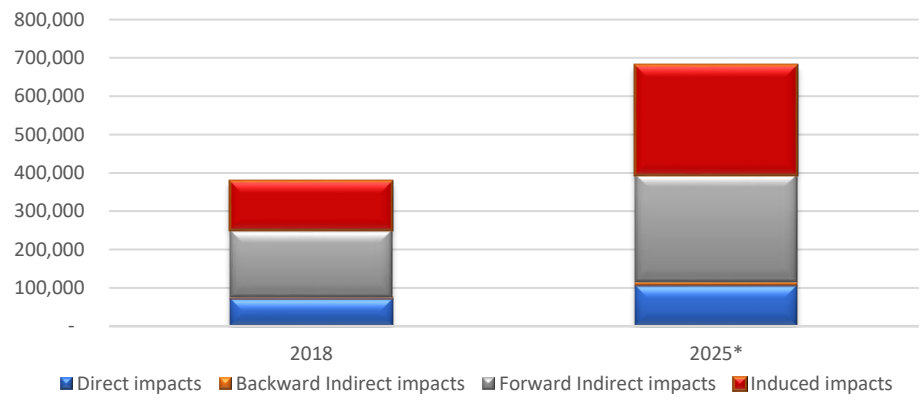
Specifically, direct impacts are those generated by the data industry itself and are measured by the revenues from data products and services sold. Indirect impacts can be distinguished in: 1) backward indirect impacts, represented by the business growth resulting from changes in sales from suppliers to the data industry; and 2) forward indirect impacts, including the economic growth depending on the adoption of data by the downstream industries, thus benefiting from optimized production and delivery processes, improved marketing and improved organization and management practices. Finally, induced impacts involve the economic activity created by additional payment of wages to staff in the data industry and its direct supply chain. A share of

these additional wages will be spent in consumer goods and services, leading to further business growth throughout the economy.

In 2018, the overall impact of the data market on the economy amounted to about € 377 bln (Fig. 3.7), with forward indirect impact accounting for the largest part (47%). Over the next 7 years, the total impact is expected to grow by 83%, reaching € 680 bln, with the greatest benefits being induced and forward indirect impacts.

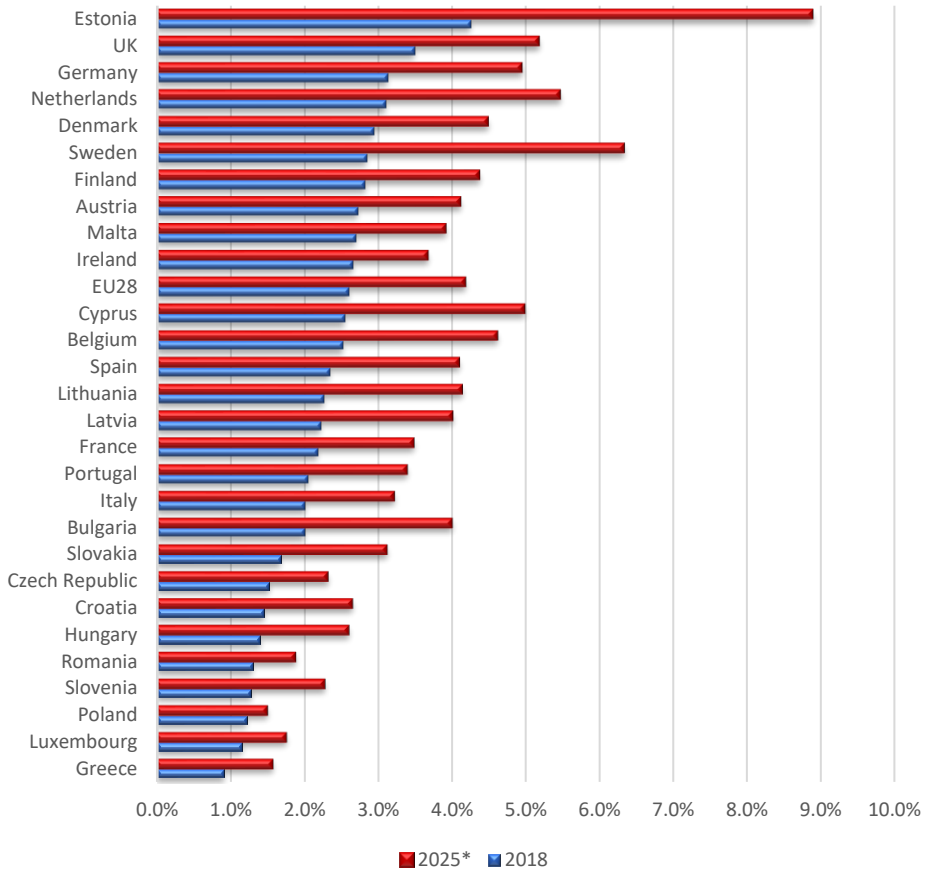
In relative terms, the impact of the data market on the EU economies is still low but is becoming more significant (Fig. 3.8), ranging from 0.9% in Greece to 4.3% in Estonia in 2018, with an EU average of 2.6%, expected to increase to 4.2% by 2025. The country with the largest relative impact by 2025, according to the estimates, is Estonia – where the data market will represent about 9% of the overall economy – followed by Sweden (6.3%) and the Netherlands (5.5%), whereas Poland will be the least affected country (1.5%).

Fig. 3.7: Data economy value in the EU



Source: I-Com elaboration on European Data Market Monitoring Tool, IDC (2019)
* Baseline scenario

Fig. 3.8: Data economy impact on GDP, by Member State



Source: I-Com elaboration on data European Data Market Monitoring Tool, IDC (2019)
* Baseline scenario

3.3. The skills challenge of Data-driven innovation

Finding value in data is about analyzing it. It requires insightful analysts and executives who ask the right questions, recognize patterns, make informed assumptions, and predict behaviour.

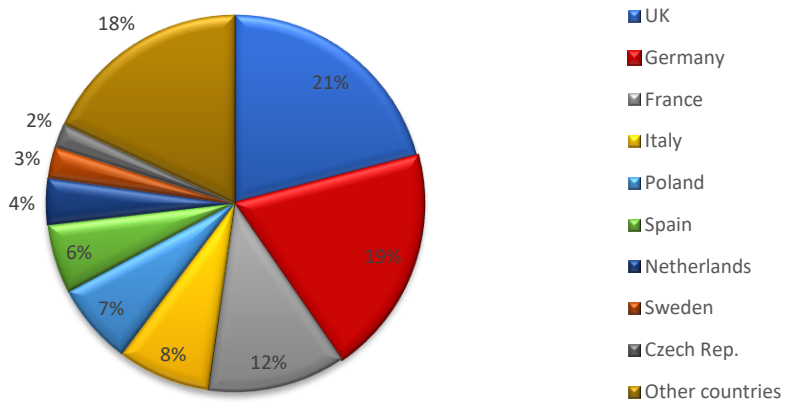
Data Analytics skills are in high demand, but supply is critically low, with employers facing severe shortages. On the demand side, since analytics is often the last step in a process, the value generated by data and their analysis can be easily computed. As a consequence, companies today are willing to invest in in-depth analyses in order to use information to optimize sales, strategies and other business functions. In every sector, companies look at data as important tools that, associated with the right analytic skills, can foster new business opportunities. On the supply side, however, the highly specialized skills needed to analyze and interpret such data are lacking.

In order to use and exploit the progressively increasing amount of data which is being produced, data analytics professionals are needed.

Data workers are defined as workers who collect, store, manage and analyze data as their primary, or important part of their activity. They are skilled in using structured and unstructured data – elaborating it to support analysis and decision-making processes – and are able to work with a huge amount of data and are familiar with emerging database technologies.

There were more than 7.2 million data workers in the EU in 2018, with 52% concentrated in three Member States - the UK, Germany and France (Fig. 3.9).

Fig. 3.9: Distribution of data workers across EU 28 (2018)

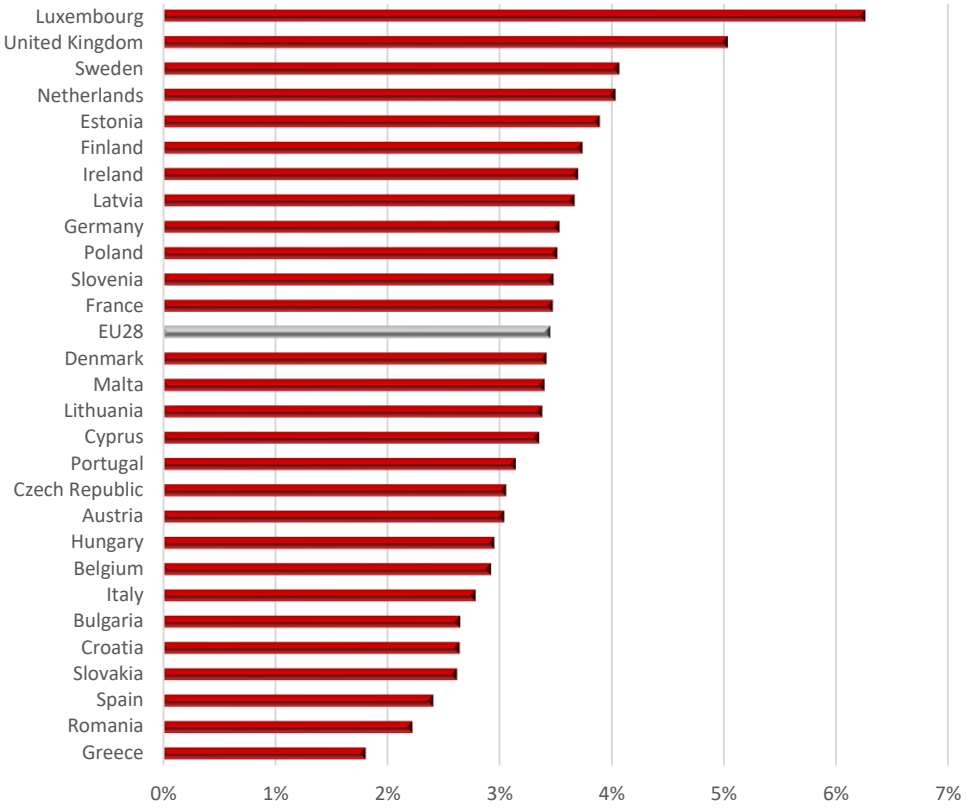


Source: I-Com elaboration on European Data Market Monitoring Tool, IDC (2019)

Data workers represent 3.41% of the total employment in the EU (Fig. 3.10). This share varies significantly by country, from 6.3% in Luxembourg to 1.8% in Greece. Two countries of the Big Five - Italy and Spain - lag behind the European average (3.4%). This relates in part to their ICT spending and, mainly, due to their industry structure where SMEs play an important role. For smaller businesses, data products and services may be less accessible compared to larger companies. In terms of employment share, the discrepancy between big and small countries tends to lose importance while structural factors, both country and industry-specific, appear to be more important.

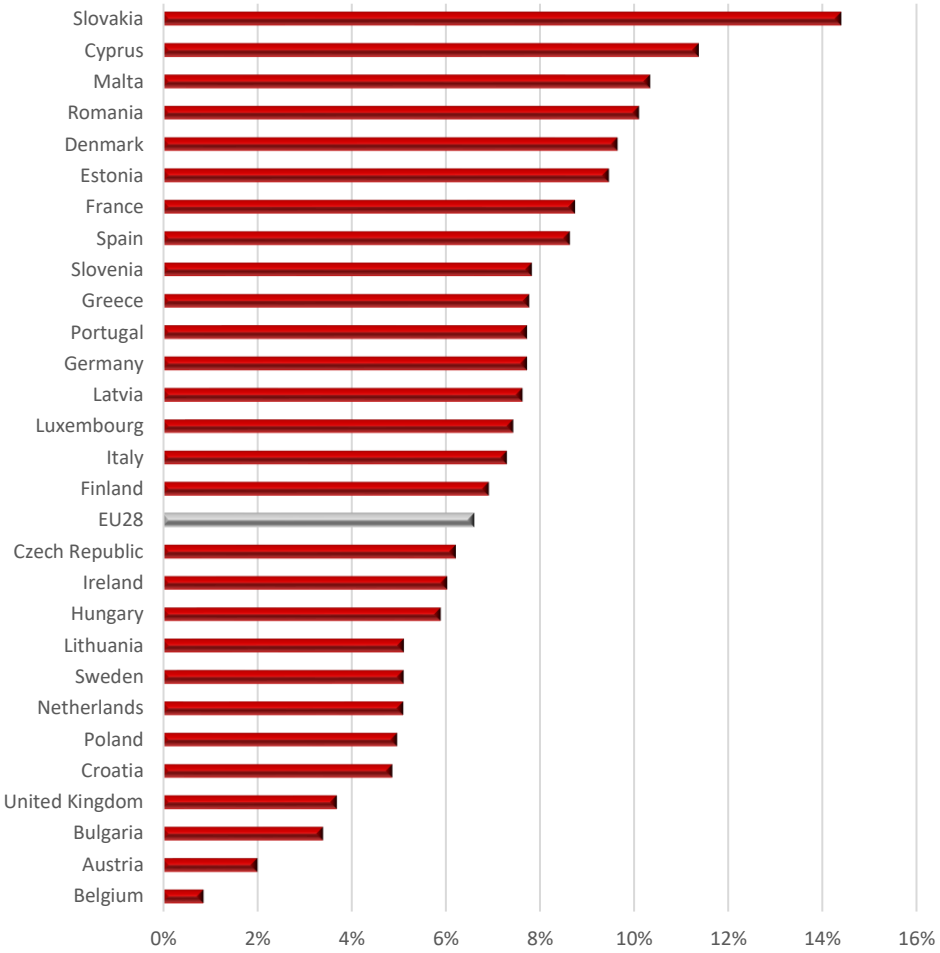
According to forecasts for 2025, the countries where the number of data workers are expected to increase the most are Slovakia (14.4% yearly), Cyprus (11.3%), Malta (10.3%) and Romania (10.1%), by a rate considerably higher than the EU average (6.6%) (Fig. 3.11).

Fig. 3.10: Share of data workers out of total employment, by Member State (2018)



Source: I-Com elaboration on data European Data Market Monitoring Tool, IDC (2019)

Fig. 3.11: Average annual growth in the number of data workers, by Member State (2018-2025)



Source: I-Com elaboration on data European Data Market Monitoring Tool, IDC (2019)

3.4. European regulatory framework on data protection

Our economy is increasingly depending on data. Data can create added value to existing services and facilitate entirely new business models, therefore it is important to remove obstacles to the free movement of non-personal data across Member States and IT systems in Europe, on one hand, and to guarantee an adequate protection of personal data, on the other hand.

Privacy regulation, in particular, is instrumental in fostering consumer trust in the digital society. The ePrivacy Directive and the General Data Protection Regulation provide the legal framework to ensure digital privacy for EU citizens.

In early 2016, the EU reformed the legal framework on data protection and issued the **General Data Protection Regulation (GDPR**) - Regulation 679/16 - entering into force on 25 May 2018, in order to protect all EU citizens from privacy and data breaches in an increasingly data-driven world, vastly different to when the 1995 Directive was presented.

The GDPR sets the foundations for the lawfulness of data processing. It clearly indicates times, contents and modalities of information, defines the rights of the interested parties (access, cancellation-forgetting, limitation of treatment, opposition, portability), fixes the key-principle "privacy by design", identifies the subjective characteristics and responsibilities of owners and data controllers, regulates international data transfers and establishes important rights such as the right to erasure ("right to be forgotten"), the right to data portability and the right of the data subject to receive the personal data in a structured, commonly used and machine-readable format with the right to transmit said data to another controller.

Considering that this regulation required Regulation (EC) 45/2001 to be adapted to the new principles and rules in order to provide a solid and consistent data protection framework in the Union, on 23 October 2018, **Regulation 2018/1725** was adopted by the European Parliament and the Council. The latter regards the protection of natural persons in the processing of personal data by Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (it will apply to the processing of personal data by Eurojust from 12 December 2019).

Conforming to the model and the general discipline established by Regulation 2016/679, the regulation identifies the principles applicable to the processing of personal data (lawfulness, correctness, transparency, adequacy, relevance, limitation) and the conditions for consent, regulating the transmission of personal data to recipients, other than Union institutions and agencies, established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680.

The Commission also launched the **proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing the Directive 2002/58/EC regulation on confidentiality and electronic communications** aimed at guaranteeing a greater protection of people's private lives and offering new business opportunities. Furthermore, the proposal, starting from the observation of the importance for Europeans to maintain the confidentiality of emails and online messages and the necessity to define a unitary protection within the Union and the applicability of the current ePrivacy Directive only to traditional telecommunications operators, provides for the extension of privacy rules to new operators supplying electronic communication services (such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, Viber). It specifies that this protection covers the contents and the metadata of electronic communications (for example, call time and location).

In order to ensure a greater user control over the settings, allowing for easy acceptance or refusal of the monitoring of cookies and other identifiers in the event of risks to privacy, the proposal provides for the simplification of the so-called "cookies provision" which has resulted in an excessive number of requests for Internet user consent.

The proposal also introduces measures against spam, prohibiting unwanted electronic communications through emails, text messages and, in principle, also telephone calls if users have not given their consent. To complete the set of protections, the proposal imposes the authors of telephone calls for commercial purposes, the obligation to show their telephone number or use a special prefix that indicates the nature of the call.

The procedure is ongoing. On 17 October 2019, the EU Council published a revised text of the ePrivacy proposal.

With regard to non-personal data, instead, on 14 November 2018, **Regulation 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union** was approved.

The regulation aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localization requirements, the availability of data to competent authorities and the porting of data for professional users. It: 1) establishes the principle of free movement of non-personal data in the Union; 2) ensures the availability of data for regulatory controls by the competent authorities, prohibiting the refusal on the basis that the data is processed in another Member State; 3) encourages the adoption of self-regulatory codes of conduct that specify information on data portability conditions; and 4) provides the designation, by each Member State, of a single point of contact which acts as a link with the contact points of the other Member States and the Commission regarding the application of the Regulation.

Together with the GDPR, this Regulation will therefore ensure a comprehensive and coherent approach to the free movement of all data in the EU.

4. THE EUROPEAN WAY TO AI

4.1. The current status and trends of the global artificial intelligence market

The global artificial intelligence market is expected to experience a massive growth in the coming years. According to the recently updated International Data Corporation (IDC) Worldwide Artificial Intelligence Systems Spending Guide, spending on AI systems will reach $97.9 bln in 2023, more than two and half times the $37.5 bln that will be spent in 2019 (Fig. 4.1). The compound annual growth rate (CAGR) for the 2018-2023 forecast period will be 28.4%.

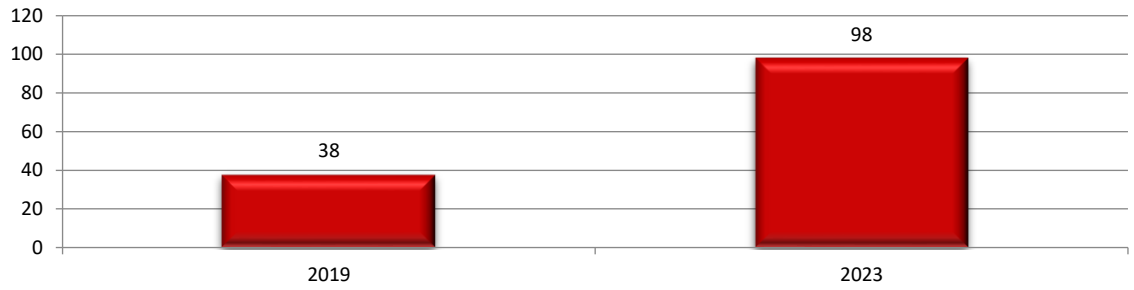
Spending on AI systems will be led by the retail and banking industries, each of which will invest more than $5 bln in 2019. Nearly half of the retail spending will go towards automated customer service agents and expert shopping advisors and product recommendation systems.

The banking industry will focus its investments on automated threat intelligence and prevention systems and fraud analysis and investigation. Other industries that will make significant investments in AI systems throughout the forecast include discrete manufacturing, process manufacturing, healthcare and professional services. Investments in AI systems continue to be driven by a wide range of use cases.

The three largest use cases – automated customer service agents, automated threat intelligence and prevention systems, and sales process recommendation and automation – will deliver 25% of all spending in 2019. The use cases that will see the fastest spending growth over the 2018-2023 forecast period are automated human resources (43.3% CAGR) and pharmaceutical research and development (36.7% CAGR). On a geographic basis, the United States is expected to deliver more than 50% of all AI spending, led by the retail and banking industries. Western Europe will be the second largest geographic region, led by banking and discrete manufacturing. China will be the third largest region for AI spending with retail, state/local government and professional services vying for the top position. The strongest spending growth over the five-year forecast will be in Japan (45.3% CAGR) and China (44.9% CAGR)[4].

[4] https://www.idc.com/getdoc.jsp?containerId=prUS45481219

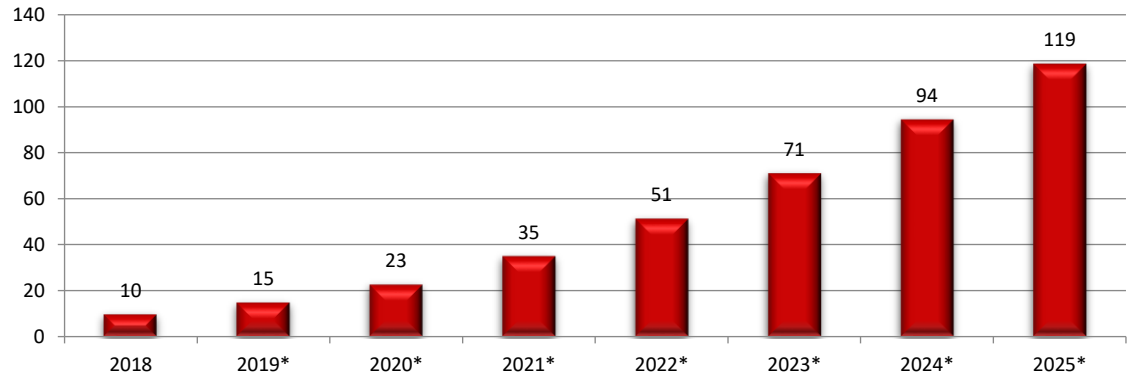
Fig. 4.1: Worldwide Spending on Artificial Intelligence Systems (billion $)



Source: IDC, 2019

The AI market is growing very fast and the interest of companies in smart technologies is becoming increasingly consolidated. According to Tractica's latest forecasts, global revenues from the implementation of AI software will increase exponentially, going from $ 9.5 bln in 2018 to $ 118.6 bln by 2025 (Fig. 4.2).

Fig. 4.2: Global revenue from the implementation of AI software (billion $)



Source: Tractica, 2019
*forecasts

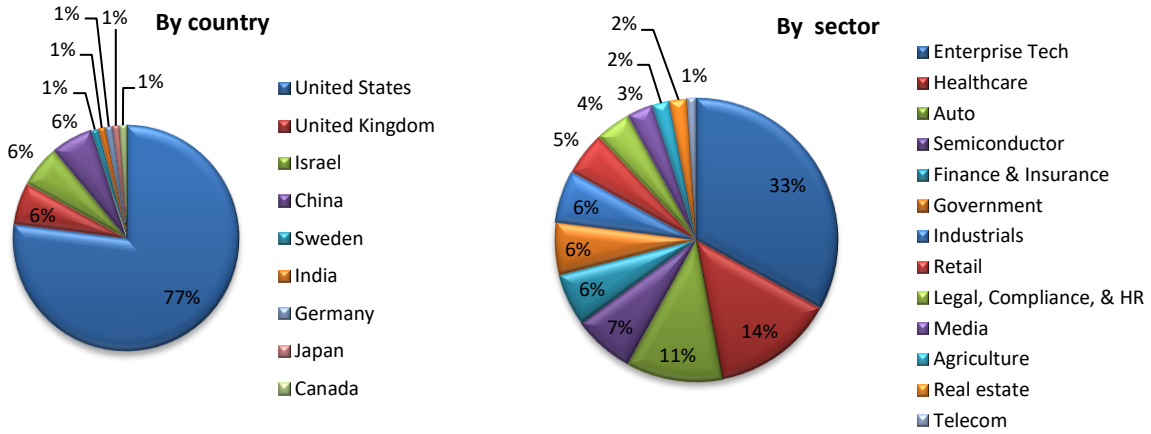
Among the various AI applications, chat-bots will become very widespread with a market size reaching about $ 1.25 bln in 2025, registering an enormous increase compared to the size of the market in 2016, which stood at $ 190.8 mln (Fig. 4.3).

Fig. 4.3: Chat-bot market worldwide (mln $)

Source: Statista, 2019

Among the main players that dominate the world scene of AI, startups account for a significant portion of innovation. According to 2019 CB Insights data, approximately 80% of the 100 most promising AI startups worldwide are based in the United States, while in the United Kingdom, Israel and China they are equally divided. Furthermore, the sectors in which there is a greater presence of highly qualified startups are business technologies, healthcare and the automotive sector (Fig. 4.4).

Fig. 4.4: The most promising 100 AI startups



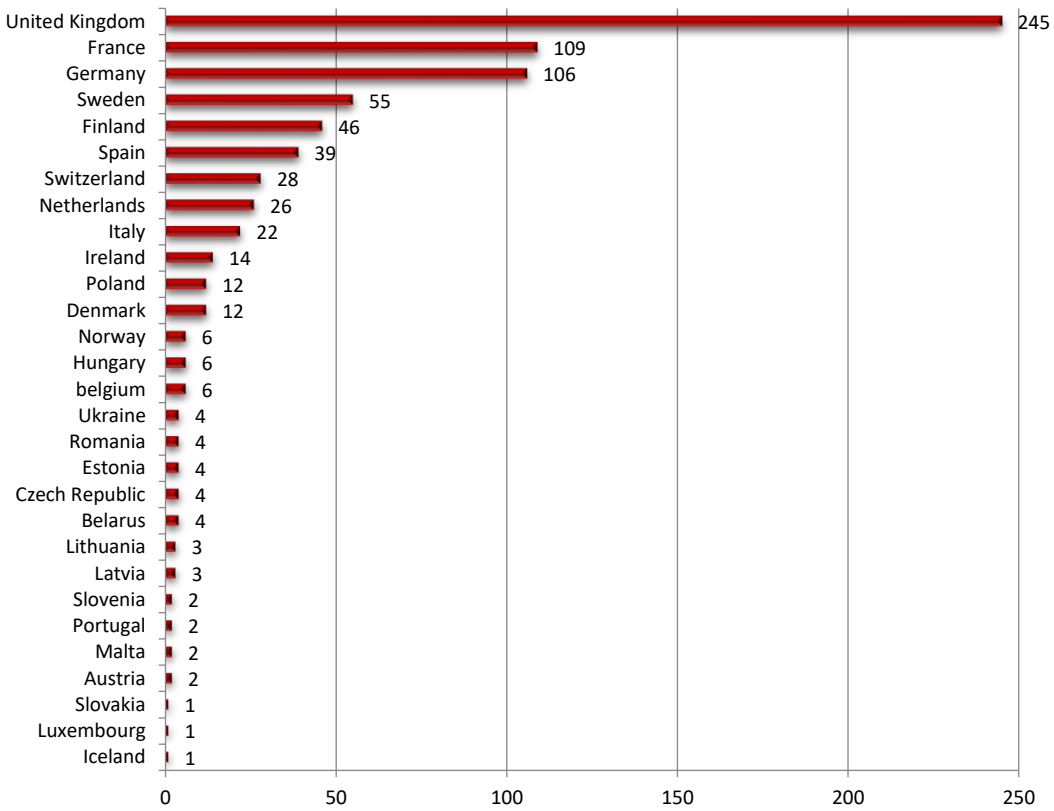
Source: I-Com elaboration on CB Insight, 2019

4.2. Artificial Intelligence in the European context

While the United States and China have a thriving AI ecosystem, Europe is still struggling to fully open up to smart technologies, although progress has been made compared to the past.

If we consider the number of AI startups in the world, the United States with about 1,400 organizations dominate the international scene, followed by China (383) and Israel (362). However, if we look at Europe as a whole, with 769 AI startups, it overtakes China. However, no European state has achieved a real critical mass, with the exception of the United Kingdom, which with 245 startups tops the European ranking, followed by France (109) and Germany (106) (Fig. 4.5).

Fig. 4.5: European startups in AI, by country



Source: I-Com elaboration on Asgard and Roland Berger, 2018

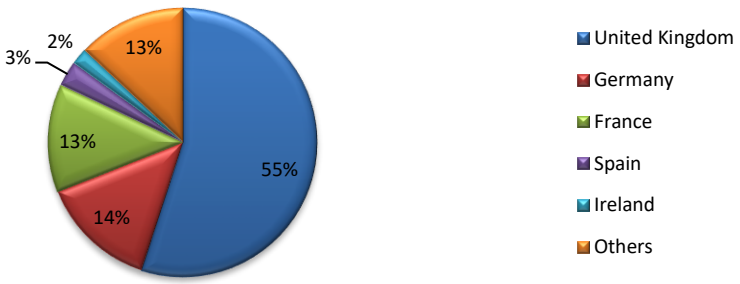
Moreover, major sectors of the European economy are weakly represented in terms of startups. The energy industry, for instance, accounts for just two 2% of European AI startups, and similar

underrepresentation could be found for the automotive industry (1%), real estate (1%), agriculture (1%) and public administration (less than 1%)[5].

If we look at the data on investments in AI startups, especially in Europe, a slightly more encouraging situation emerges (at least in terms of trends).

In fact, private equity investment in AI has accelerated since 2016, with the amount of private equity invested doubling from 2016 to 2017. In total, it is estimated that more than $ 50 bln was invested in AI startups during the period 2011 through to mid-2018. In this context, the European Union accounted for 8% of global AI equity investment in 2017. This represents an important increase for the region as a whole, which accounted for just 1% of this investment in 2013. However, investment levels vary widely among the Member States. The British startups received 55% of EU total investment over the period 2011 to mid-2018, followed by German (14%) and French ventures (13%), implying that the remaining 25 countries shared less than 20% of all private AI equity investments received in the European Union[6] (Fig. 4.6).

Fig. 4.6: Private equity investments in AI startups based in the EU, 2011 to mid-2018



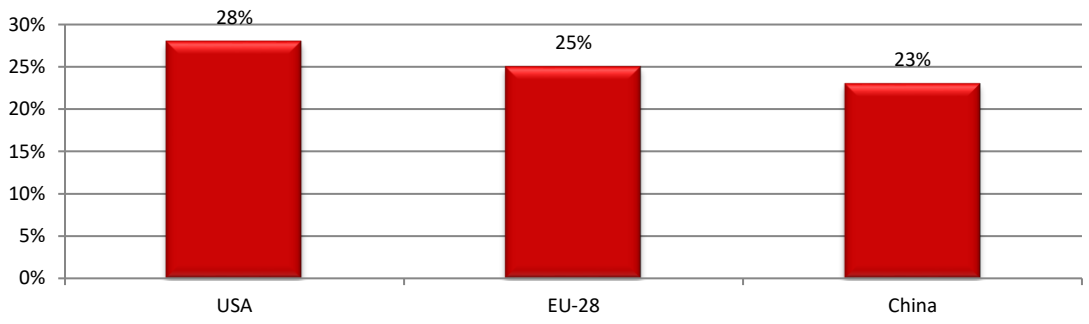
Source: OECD

Furthermore, according to a study by the Joint Reseach Center of the European Commission, although the EU is among the geographical areas with the largest number of players active in AI - with 25% of the total, just below the United States (28%) and above China (23%) (Fig. 4.7) - European companies are still not inclined to adopt more advanced machine learning techniques as well as AI tools such as intelligent workflows, cognitive agents and natural language processing

[5] https://asgard.vc/wp-content/uploads/2018/05/Artificial-Intelligence-Strategy-for-Europe-2018.pdf
[6] OECD, Private Equity Investment in Artificial Intelligence, 2018

systems. Within the EU, the countries with the most AI players are the UK (25%), Germany (15%) and France (11%)[7].

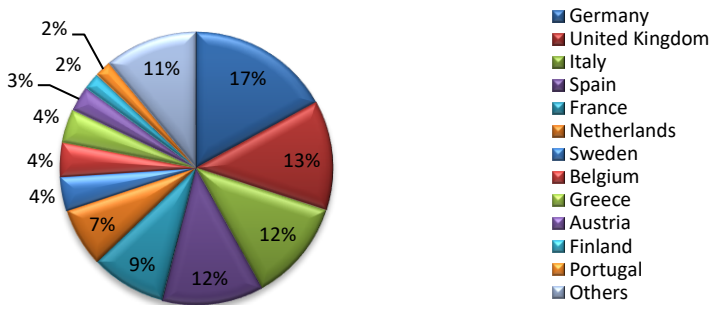
Fig. 4.7: AI Players (% of world total; 2009-2018)



Source: European Commission, Joint Research Center

Among the AI research projects funded under the FP7 and Horizon 2020 projects, Germany ranks first with a 17% share, followed by the United Kingdom (13%), Italy and Spain (12%) (Fig. 4.8).

Fig. 4.8: Distribution of EU players in EU-funded AI research projects, 2009-2018



Source: European Commission, Joint Research Center

Finally, I-Com elaborated a synthetic index to give an idea of the level of preparedness for AI in the EU countries. The I-Com index is based on 13 variables that are closely related to the topic of

[7] European Commission, "Artificial Intelligence. A European perspective", 2018

artificial intelligence. The variables are listed below and refer to the adoption of technology, skills, security and infrastructure:

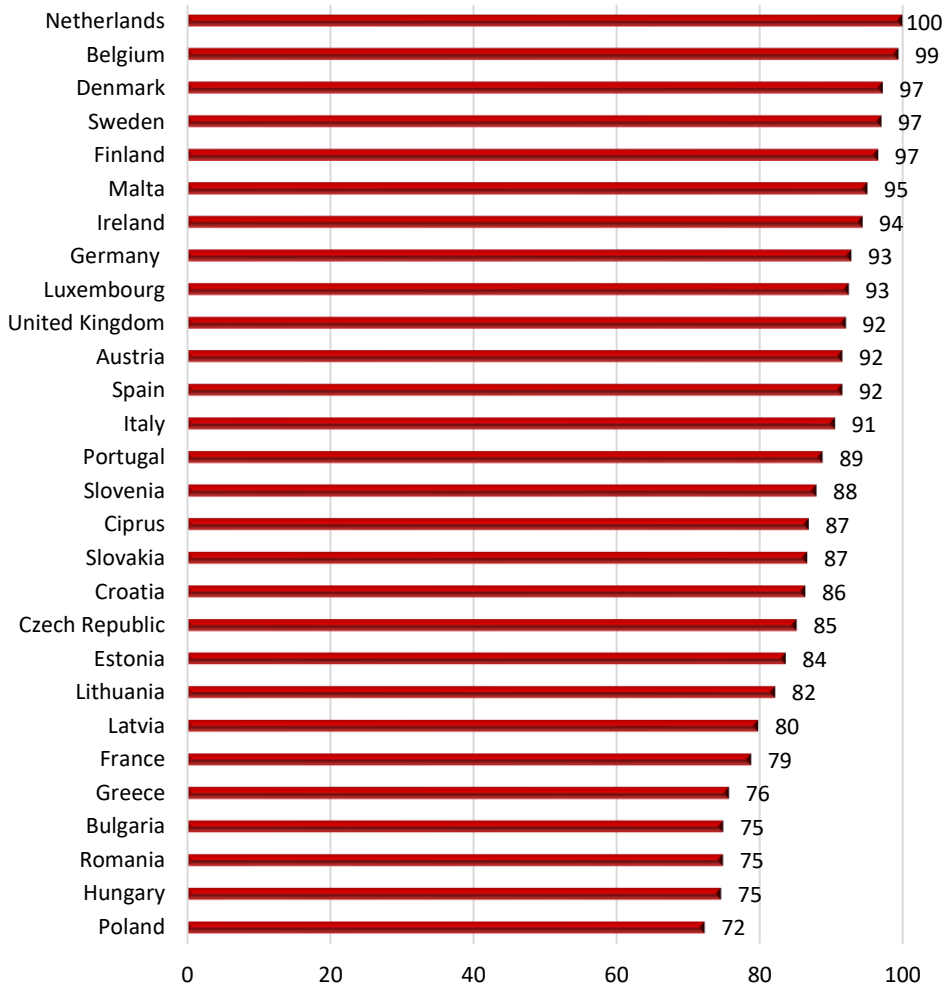
1. Enterprises that share internally electronic information with an ERP
2. Enterprises using Radio Frequency Identification (RFID) technologies
3. Enterprises buying Cloud Computing services of high sophistication
4. Enterprises using software solutions like Customer Relationship Management (CRM)
5. Enterprises analyzing Big Data from any data source
6. Enterprises using 3D printing
7. Enterprises using robots
8. Share of ICT specialists out of total employment
9. Share of data workers out of total employment
10. Share of STEM graduates
11. Share of companies with an ICT security policy
12. NGA broadband coverage of the population
13. 4G coverage of the population

Each variable was appropriately weighted and an average of the variable values was calculated for each country. The obtained values were finally normalized relative to the best performer country, so as to establish a ranking from 0 to 100.

With a score of 100, the Netherlands leads the ranking, showing the best enabling conditions for the development of an AI ecosystem. Followed by Belgium (99), Denmark, Sweden and Finland with a score of 97. The northern countries share a good level of technology adoption - above the EU average - and an excellent level of infrastructure development.

Most Eastern European countries lag behind, due to low levels of AI technology adoption and skills (Fig. 4.9).

Fig. 4.9: I-Com Index 2019 on the level of preparedness for AI across EU countries



Source: I-Com Elaboration on European Commission, Eurostat and IDC

4.3. Analysis of European AI initiatives

Artificial intelligence is one of the most important digital phenomena being able to deeply impact on all economic sectors and offer new opportunities for citizens, public administrations and companies. However, there are a lot of socio-economic, legal and ethical problems to be carefully addressed to ensure competitiveness and to shape the conditions for its development and use.

On 16 February 2017, the European Parliament adopted a **resolution with recommendations to the Commission on Civil Law Rules on Robotics**, describing the benefits related to the increasing

use of AI in terms, for example, of safeguarding workers in the more difficult or dangerous professions, but also, in general, the impact on the job market and the skills required from workers.

In May 2017, the Commission published its **mid-term review of the Digital Single Market Strategy** underlining the importance of building on Europe's scientific and industrial strengths, as well as on its innovative startups, to be in a leading position in the development of AI technologies, platforms and applications.

On 9 March 2018, the Commission launched a selection for the creation of an **AI working group** with the task, among other things, of preparing a proposal for guidelines on ethical development and use of AI in compliance with the EU Charter of Fundamental Rights, considering issues such as fairness, security, transparency and the future of the world of work and democracy. On the same date, the Commission also opened a call for the formation of **a group of experts on damage and new technology responsibility** with the task of advising the Commission on the applicability of the Directive on damage liability regarding defective products to traditional products and new technologies.

Considering the importance of AI and the tremendous opportunities for growth connected to its deployment and use, on 10 April 2018, 25 European countries[8] signed a **Declaration of Cooperation on Artificial Intelligence**. Above all, the Member States agreed to work together on the most important issues raised by AI, to ensure Europe's competitiveness in the research and deployment of AI and deal with social, economic, ethical and legal questions. It was endorsed by the European Council in June 2018.

On 25 April 2018, the European Commission published a **communication putting forward a European approach to artificial intelligence** based on three pillars: 1) being ahead of technological developments and encouraging uptake by the public and private sectors with the Commission increasing its annual investments in AI by 70% under the research and innovation program Horizon 2020, reaching €1.5 bln for the period 2018-2020, connecting and strengthening AI research centers across Europe and supporting the development of AI applications in key sectors and an "AI-on-demand platform" that will provide access to relevant AI resources in the EU for all users; 2) preparing for socio-economic changes brought about by AI supporting business-education partnerships to attract and keep more AI talent in Europe and training and retraining schemes for professionals, also encouraging the modernization of Member State education and training systems and foreseeing changes in the labor market and skills mismatching; and 3) ensuring an appropriate ethical and legal framework.

[8] Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, the UK, Norway

On 7 December 2018, the Commission published the Coordinated Plan on AI resulting from the work of the 25 Member States which signed the Declaration of Cooperation on Artificial Intelligence in April 2018. It details actions to be started in 2019-2020 and prepares the ground for activities in the following years. It will be reviewed and updated annually. Considering that only five Member States had already adopted a national AI strategy with a specific budget (France, Finland, Sweden, the UK and Germany) while others (Denmark, Luxembourg, the Netherlands, Ireland and Norway) include AI related actions in their broader digitization strategies, the document has provided a strategic framework for national AI strategies encouraging the adoption of them by mid-2019. This Plan identifies some goals and actions: 1) reinforcing cooperation with the private sector; 2) strengthening excellence in trustworthy AI technologies and broader dissemination; 3) adapting learning and training programs and systems to better prepare society for AI; 4) building up the European data space essential for AI in Europe, including for the public sector; 5) developing ethics guidelines with a global perspective and ensuring an innovation-friendly legal framework; and 6) better understanding security-related aspects of AI applications and infrastructure.

On 12 February 2019, the European Parliament adopted a Resolution on a comprehensive European industrial policy on artificial intelligence and robotics. Considering that AI is one of the strategic technologies for the 21st century, both globally and in Europe, bringing about positive changes for the European economy, enabling innovation, productivity, competitiveness and wellbeing and the necessity to adopt a coordinated approach at a European level to compete with the massive investments made by third countries, especially the US and China, the resolution underlines the importance of ensuring a trusted ecosystem for AI technology development. It also highlights that there are strong ethical, psychological and legal concerns about the autonomy of robots, their obvious lack of human empathy and their impact on the doctor-patient relationship, which have not yet been properly addressed at EU level. This particularly regards the protection of patients' personal data, liability, and the new economic and employment relationships that will emerge.

On 9 April 2019, the High-Level Expert Group on AI presented the "Ethics Guidelines for Trustworthy AI", following the publication of the guidelines' first draft in December 2018 on which more than 500 comments were received through an open consultation. The document sets out a framework for achieving trustworthy AI aiming to offer guidance to all stakeholders identifying a list of ethical principles, by providing guidance on how such principles can be operationalized in socio-technical systems. Guidance is provided in three layers of abstraction, from the most abstract in Chapter I to the most concrete in Chapter III, closing with examples of opportunities and critical concerns raised by AI systems.

It underlines that trustworthy AI should be: 1) **lawful**, complying with all applicable laws and regulations; 2) **ethical**, ensuring adherence to ethical principles and values; and 3) **robust**, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm.

The Guidelines are divided into 3 chapters: a) Foundations of Trustworthy AI, setting the ethical principles that must be adhered to in order to ensure ethical and robust AI. Namely, the document highlights the importance to ensure the respect for human dignity, freedom of the individual, democracy, justice and the rule of law, to guarantee equality, non-discrimination and solidarity and the safeguarding of citizens' rights. The Guidelines identify four ethical principles, rooted in fundamental rights, which must be respected in order to ensure that AI systems are developed, deployed and used in a trustworthy manner, specified as ethical imperatives and, namely: 1) respect for human autonomy; 2) prevention of harm; 3) fairness; and 4) explicability; b) Realizing Trustworthy AI, translating these ethical principles into 7 key requirements that AI systems should implement (human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non- discrimination and fairness, societal and environmental wellbeing and accountability) and meet throughout their entire life cycle, offering both technical and non-technical methods for their implementation; c) Assessing Trustworthy AI, setting out a concrete and non-exhaustive Trustworthy AI assessment list to operationalize the requirements of Chapter II, offering AI practitioners practical guidance.

Finally, on 26 June 2019 the High-Level Expert Group on AI (AI HLEG) presented the report "***Policy and investment recommendations for trustworthy Artificial Intelligence***" representing the second deliverable of the Group, after Ethics Guidelines for Trustworthy AI published on 8 April 2019. It is a very interesting document which identifies 4 major areas of impact - Humans and Society, Private Sector, Public Sector and Research and Academia - and indicates which impact to achieve with AI and identifies the enablers for trustworthy AI (infrastructures, skills and education, appropriate governance and regulatory framework and a lucrative funding and investment climate), providing a number of recommendations on how this can be accomplished.

Specifically, it underlines the importance of encouraging investments, research and development on the impact of AI on individuals and society and emphasizes the importance of: 1) increasing knowledge and awareness of AI through digital literacy and courses (e.g. MOOCs) across Europe providing elementary AI training, supporting and further developing basic education on AI and digital literacy, particularly in primary, secondary and tertiary education systems, as well as beyond, creating an AI competence framework for individuals (including a focus on the core skills required), institutionalizing a dialogue between policy-makers, developers and users of AI technology, informing the public at large about free available resources on AI that they can use to learn and experiment with (e.g. algorithms and data), to discuss (e.g. via blogs) and to share best

practices (through a platform, for example) and establishing a yearly European AI Awareness Day; 2) protecting the integrity of humans, society and the environment, refraining from disproportionate and mass surveillance of individuals, countering commercial surveillance of individuals (particularly consumers) and society, giving consideration to power asymmetries between institutions, businesses and individuals arising from the growth of digital devices and systems and the rapid expansion of digital data that they generate, introducing a mandatory self-identification of AI systems and fostering the development of AI solutions that address sustainability challenges; 3) promoting a human-centric approach to AI at work, promoting the research, development and deployment of human-centric AI systems in work contexts without stifling socially beneficial innovation, encouraging automation of dangerous tasks and when humans are put at risk, applying a process of representation, consultation and, where possible, co-creation (where workers are involved in the discussion around AI production, deployment or procurement process to guarantee that the systems are useable and that the worker still has sufficient autonomy and control, fulfilment and job satisfaction), encouraging re-skilling and up-skilling of workers and establishing a fully-fledged European transition fund to help manage the AI transformation in a socially responsible way; 4) ensuring that no one is left behind, introducing a duty of care for developers of consumer-oriented AI systems to ensure that these can be used by all intended users (in particular, users with disabilities, particularly when used in public services), fostering a universal design approach, encouraging the development of AI tools and applications targeted to help vulnerable demographics and establishing a European Strategy for Better and Safer AI for Children.

With regard to the private sector, instead, the document highlights the need for: 1) boosting the uptake of AI technology and services across sectors in Europe, allocating significant resources in the InvestEU program to support the transformation of European enterprises to AI-enabled solutions, creating an easy avenue for startups and SMEs to funding and advice, fostering the availability of legal and technical support to implement Trustworthy AI solutions that comply with the Ethics Guidelines, encouraging companies to form partnerships with training programs addressing all levels of AI training; 2) fostering and scaling AI solutions by enabling innovation and promoting technology transfer, supporting the development and growth of AI technology firms in Europe, facilitating the transition of AI solutions from research labs to testing environments and to commercial markets, creating an EU-wide network of AI business incubators that connect academia and industry and stimulating – through the Horizon Europe Program - beneficial innovation by funding EU hackathons, competitions and industry challenge driven research missions in AI across various sectors; 3) setting up public-private partnerships to foster sectoral AI ecosystems, conducting, in the short term, a sectoral-based in-depth analysis of several selected

AI ecosystems and, in the medium term, setting up Sectoral Multi-Stakeholder Alliances (SMUHAs) for strategic sectors in Europe to build their AI ecosystems with the relevant stakeholders.
With regard to the public sector, the document recommends providing human-centric AI-based services for individuals offering to individuals the possibility, if requested, to interact with a human interlocutor, catalyzing AI development in Europe, fostering digitalization by transforming public data into a digital format, making strategic use of public procurement to fund innovation and ensure trustworthy AI, safeguarding fundamental rights in AI-based public services and protect societal infrastructures, by ensuring the application of the Ethics Guidelines for Trustworthy AI to AI systems deployed by the public sector.
Finally, concerning research and academia, the document underlines the necessity to develop and maintain a European strategic research roadmap for AI, focusing on areas of strategic value and opportunities, ensuring AI solutions that meet the Trustworthy AI principles and requirements, providing dedicated, significant and long-term research funding, creating incentives and support for interdisciplinary and multi-stakeholder research, simplifying and streamlining the structure of research funding instruments, creating the conditions for talents to find Europe attractive as a research environment, creating, strengthening and supporting additional Centres of Excellence (CoEs) that address strategic research topics and become a European level multiplier for a specific AI topic and, finally, encouraging cooperation at all levels.

5. THE IMPACT OF AI ON THE LABOR MARKET

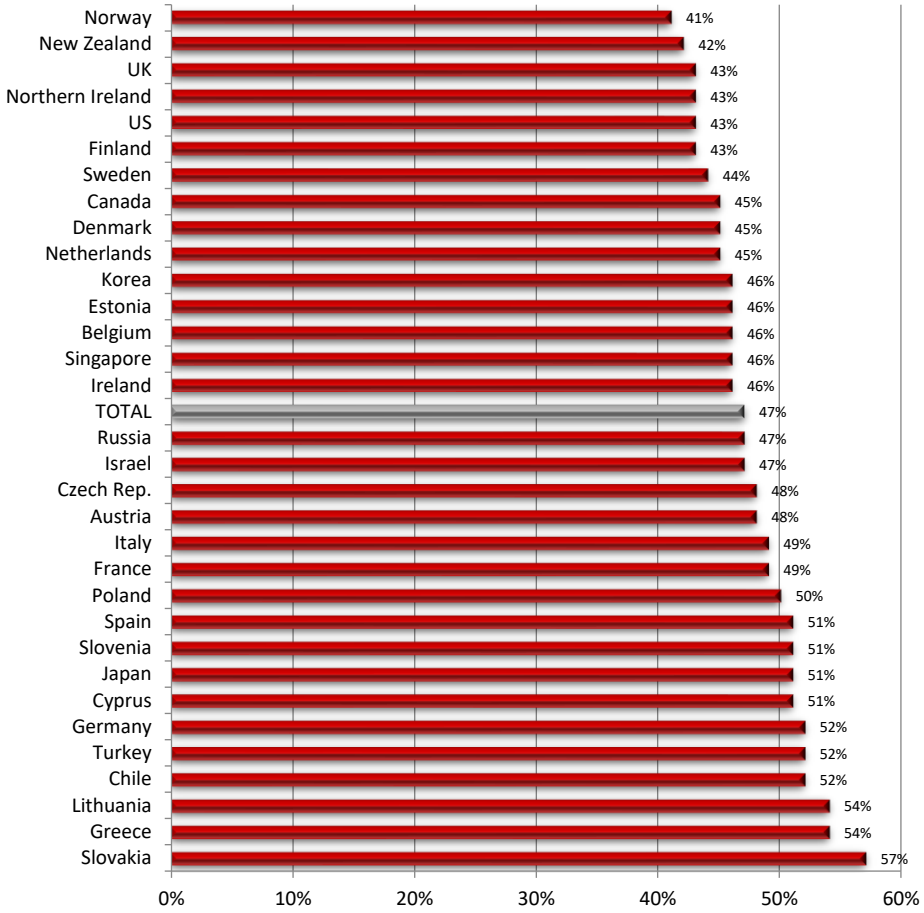
5.1. Labor organization and new jobs in the AI era: opportunities and risks of the technological evolution

In order to harness the transformative potential of the Fourth Industrial Revolution, business leaders across all industries and regions will increasingly be called upon to formulate a comprehensive workforce strategy ready to meet the challenges of this new era of accelerating change and innovation. Policy-makers, educators, labor unions and individual workers likewise have much to gain from deeper understanding of the new labor market.

Global labor markets are set to undergo significant transformations over the coming years. A cluster of emerging roles will gain importance, while another cluster of job profiles is set to become increasingly redundant. According to a study from the OECD[9], for an overall sample of 32 countries analyzed, the average job is estimated to have 47% probability of being automated (Fig. 5.1). However, there is a large variation in the degree of automatability across countries, ranging from 41% in Norway to 57% in Slovakia. The occupational groups that have the highest probability of becoming automated typically do not require specific skills or training. At the other end of the spectrum are occupations that require a high level of education and training and which involve a high degree of social interaction, creativity, problem-solving and caring for others (professionals, managers, but also personal care workers). The industries with a higher risk of automation belong mostly to the primary and the secondary sectors (Fig. 5.2). Few service industries – notably, postal and courier services, food and beverage services, land transport, waste collection and treatment, and services to buildings and landscape – face a high risk of automation. At the opposite end of the ranking, the industries with a low average probability of being automated all belong to the service sector and the category of Knowledge Intensive Business Services. Education is indeed the least likely automatable sector.

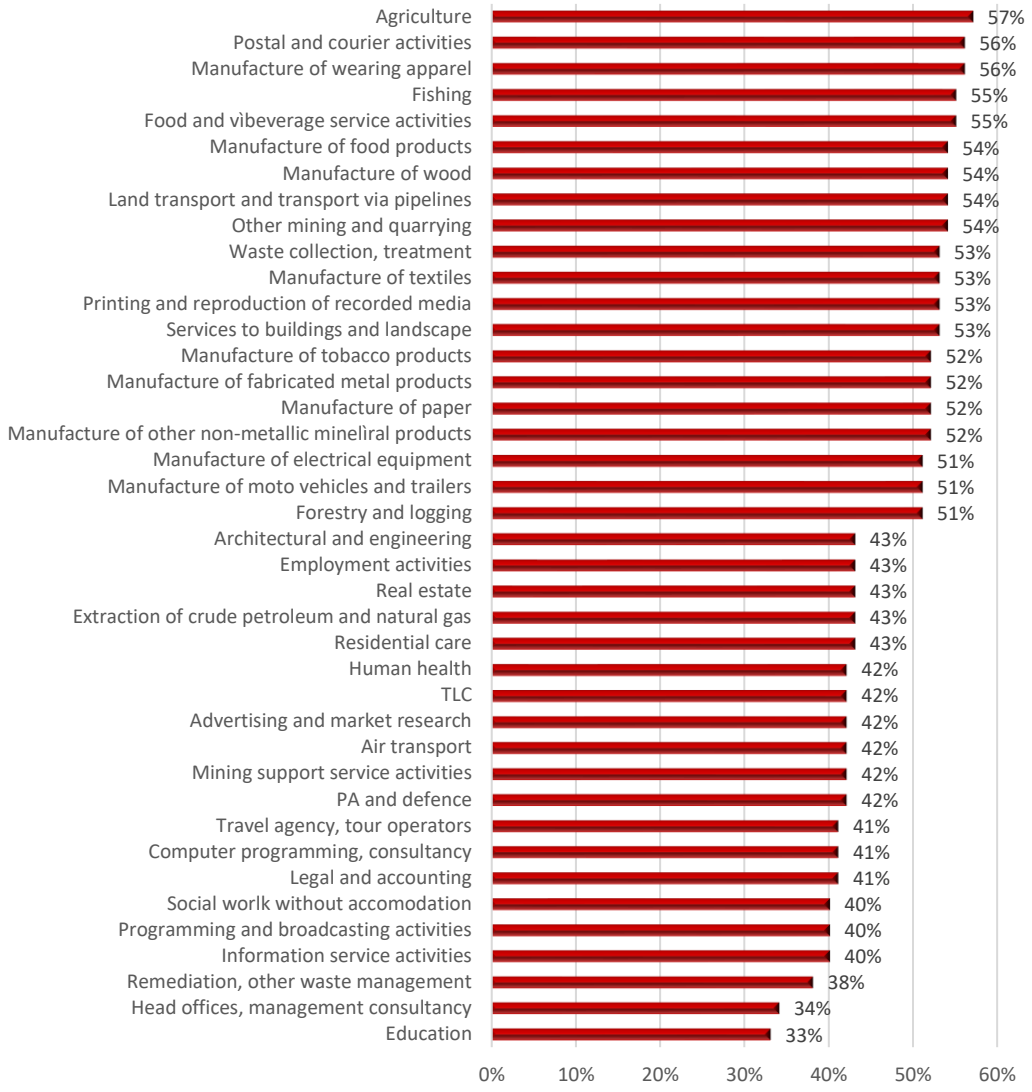
[9] L. Nedelkoska, G. Quintini, "Automation, skills use and training", 2018

Fig. 5.1: Job automation risk, by country (2018)



Source: OECD (2018)

Fig. 5.2: Average probability of automation by industry



Source: OECD (2018)

According to a World Economic Forum (WEF) study[10], however, while 75 million jobs may be displaced, 133 million additional new roles may emerge. Automation is expected to lead to some reductions in the full-time workforce, to extend the workforce to new productivity-enhancing roles and to create new roles in enterprises. Among the roles that are set to experience an increasing demand are Data Analysts and Scientists, Software and Applications Developers, and Ecommerce and Social Media Specialists that are significantly based on and enhanced by the use of technology.

[10] WEF, "The future of jobs 2018", (2018)

Also expected to grow are roles that leverage distinctively human skills such as Customer Service Workers, Sales and Marketing Professionals, Training and Development, People and Culture, and Organizational Development Specialists as well as Innovation Managers. Moreover, technology will also create new tasks — from app development to piloting drones to remotely monitoring patient health — opening up opportunities for work never previously done by human workers. Thus, there will be an accelerating demand for a variety of new specialist roles related to understanding and leveraging the latest emerging technologies - AI and Machine Learning Specialists, Big Data Specialists, Process Automation Experts, Information Security Analysts, User Experience and Human-Machine Interaction Designers, Robotics Engineers and Blockchain Specialists. On the other hand, the jobs expected to become increasingly redundant are routine-based, middle-skilled white-collar roles — such as Data Entry Clerks, Accounting and Payroll Clerks, Secretaries, Auditors, Bank Tellers and Cashiers — that are susceptible to advances in new technologies and process automation.

Most importantly, automation often occurs at the level of specific work tasks, not at the level of whole jobs. Therefore, the most important question should be not to what extent automation will affect current employment numbers, but how a new division of labor between human workers, robots and algorithms can be supported.

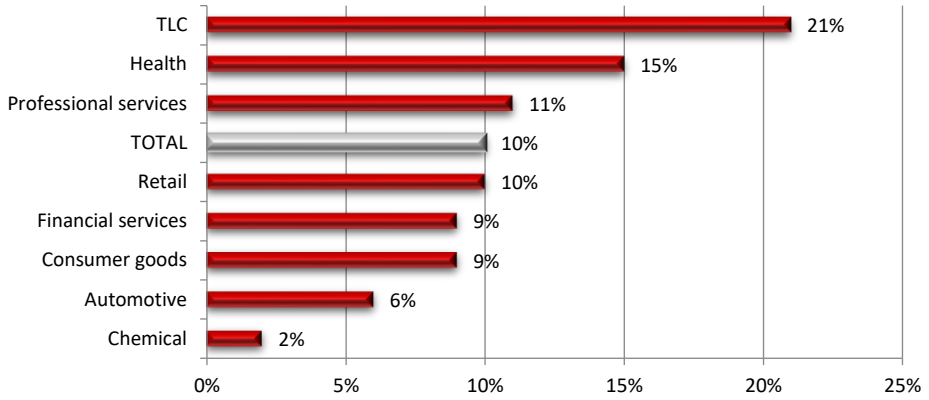
The rise of workplace automation has the potential to vastly improve productivity and augment the work of human employees. Automation technology can, indeed, help remove the burden of repetitive administrative work and enable employees to focus on solving more complex issues while reducing the risk of error, allowing them to focus on value-added tasks. Nevertheless, automation will not necessarily result in the replacement of the human workforce, as often suggested. On the contrary, the automation of some job tasks can be used to enhance the human workforces' comparative strengths, thus enabling employees to extend their potential and competitive advantage. Once they are freed of the need to perform routinized, repetitive tasks, human workers, often in complementing technology, can accomplish value-creating activities, thus turning automation in augmentation.

In order to really exploit human-machine collaboration opportunities, companies need to implement a strategic repositioning of the human resource function and to expand organizational capabilities in data analysis and workforce analytics. On the other hand, workers need to re-focus their work on high-value activities and to equip themselves with the appropriate skills.

Accenture[11] estimates that if companies properly invested in AI and in human-machine collaboration, they could boost employment by 10% (Fig. 5.3), with the largest benefits in the TLC, health, professional services and retail industries.

[11] Accenture, "Reworking the Revolution: Are you ready to compete as intelligent technology meets human ingenuity to create the future workforce", 2018

Fig. 5.3: Changes in employment



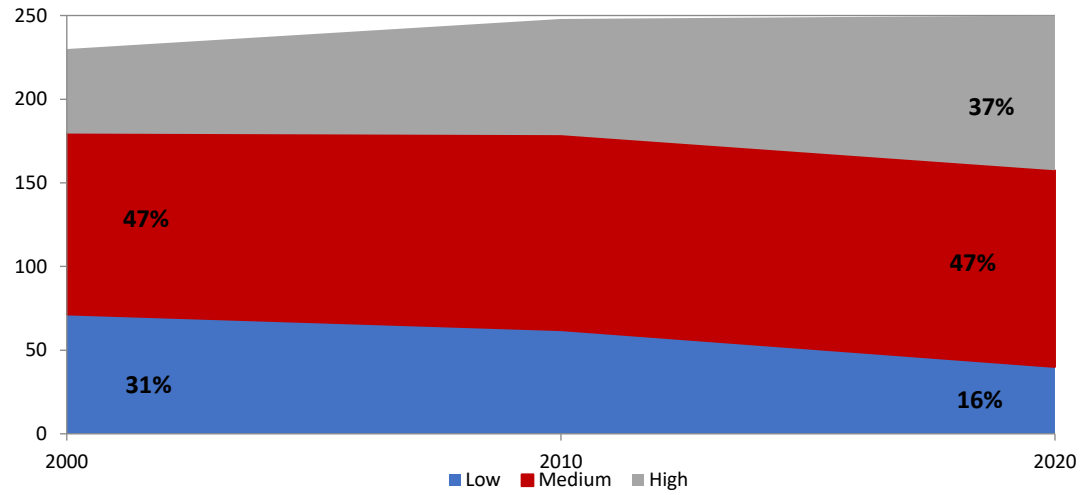
Source: Accenture (2018)

5.2. Skills and the role of education and training

Current shifts underway in the workforce will displace some workers while, at the same time, create new opportunities for others. Workers with appropriate skills may see their wages and job quality increase considerably. Conversely, even if automation only affects a subset of the tasks within their job role, workers lacking skills needed to adapt to new technologies and to move on to higher value tasks may see their wages and job quality undermined by technology steadily eroding the value of their job.

Occupations requiring strong social, interpersonal skills and non-routine analytical skills have grown dynamically since 1980 with consistent wage growth. Even in the tech industry, it is jobs that require both technical and interpersonal skills that are on the rise. Cultures of sharing, negotiating with others and finding compromises seem to be what will make the difference. Europe's advantage in the future highly automated world of work lies in its creativity and highly skilled workforce. In 2000, less qualified jobs numbered about 65 million, by 2020 they will be less than 40 million (-40%), just 16% of total employment (31% in 2000). On the contrary, highly qualified work, representing less than 20% of employment in 2000, will account for 37% in 2020, with 90 million jobs overall (Figure 5.4).

Fig. 5.4: Labor Force by Level of Qualification in the European Union



Source: European Commission (2016)

In the coming years, the skills required to perform most jobs will have markedly changed. According to the World Economic Forum, over the 2018–2022 period, only 58% of skills are expected to remain stable, meaning an average shift of 42% in the required workforce skills, identifying a continued fall in demand for manual skills and physical abilities and, on the other hand, a decrease in demand for skills related to the management of financial and other resources, as well as basic technology installation and maintenance skills. Skills continuing to grow include analytical thinking and innovation as well as active learning and learning strategies. According to the WEF's findings, employees most in need of reskilling and upskilling are least likely to receive such training. According to other research, currently, only about 30% of employees in today's job roles with the highest probability of technological disruption have received any kind of professional training over the past 12 months. In addition, they are on average more than three times less likely than employees in less exposed roles to have participated in any on-the-job training or distance learning and about twice less likely to have participated in any formal education[12]. To date, reskilling has been regarded by employers as a narrow strategy focused on specific subsets of employees, not as a comprehensive strategy to drive workforce transformation.

The development of AI models requires very high levels of competence in several areas. Work in this area requires advanced levels of scientific mathematical and technical skills that are not easy to acquire, as well as a good understanding of statistics and computer architectures and

[12] See note 2.

programming tools[13]. The largest influence of AI adoption is the development of complementary human skills as AI technologies evolve. The two biggest barriers to AI adoption in European companies are linked to having the right workforce in place. The first barrier relates to the ability in using ICT tools at work. The second barrier relates to companies' needs for skills to provide new AI applications and services, such as AI coding and analytic expertise[14]. Not by chance, companies find it particularly difficult to fill job openings for engineers, technicians and analytic expertise. More in general, the share of enterprises having hard-to-fill vacancies for jobs requiring ICT specialist skills increased from 3% in 2015 to 5% in 2018[15].

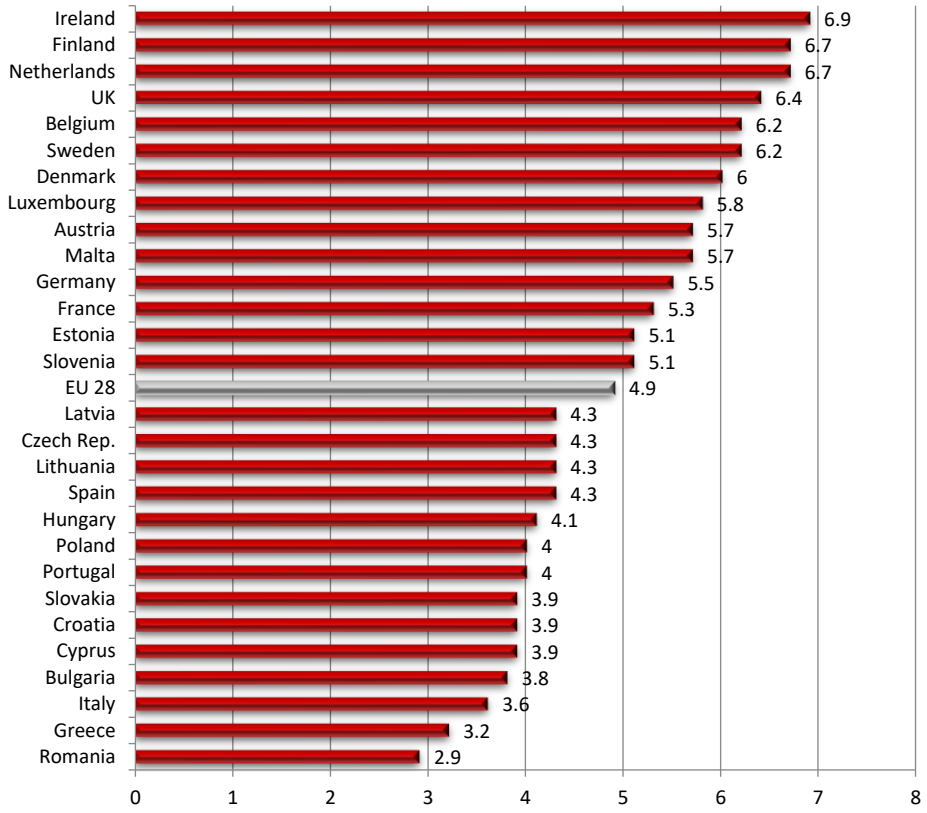
A key issue is the need for horizontal skills. For instance, translating data – a key resource to AI - into economic value entails more than just technical skills. It involves a new way of thinking, the development of encompassing skills and the ability to rapidly generate new operating models. As described by the European Commission[16], the right skills needed to "future ready" professionals derive from a combination of the T-shape metaphor together with the leadership skill triangle, resulting in innovators with the necessary high-tech talent and leadership skills. They display:

- Strategic Leadership: to lead inter-disciplinary staff, and influence stakeholders across functional and geographic boundaries;
- Business Savviness: to innovate business and operating models, delivering value to organizations;
- High-tech Savviness: to envision and drive change for business performance, exploiting the innovation opportunities in high-tech trends.

The European Commission published the High-tech Leadership Index, based on 24 indicators belonging to the following four domains: e-leadership education, proportion of the workforce with e-leadership potential, structural variables that permit opportunities of e-leadership to be exploited and e-leadership enabling policies or other drivers. It measures the factors likely to affect demand and supply for e-leadership skills in each country. Ireland, the Netherlands, Finland, the UK, Sweden, Belgium and Denmark are the frontrunners, with performance more than 20% above the EU average (Fig. 5.5), whereas Cyprus, Croatia, Slovakia, Bulgaria, Italy, Greece and Romania are at the other end of the ranking.

[13] European Commission, "Artificial Intelligence. A European perspective", 2018
[14] McKinsey & Company, "Notes from the AI frontier: Tackling Europe's gap in digital and AI", 2019.
[15] Eurostat (2019).
[16] European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, "High-Tech Leadership Skills for Europe", 2017

Fig. 5.5: High-tech Leadership Index



Source: European Commission (2017)

The European Commission estimates that there are 800,000 high-tech leaders in the EU, but a total of an additional 450,000 will be needed by 2025. Of these, about 86% will be leaders in the field of digital leadership, the remaining 14% in the field of KETs[17]. Concerning the former, Big Data, Internet of Things and robotics-cognitive systems combination are the most disruptive technologies, which will produce the largest demand – and then will face the greatest lack – of skills.

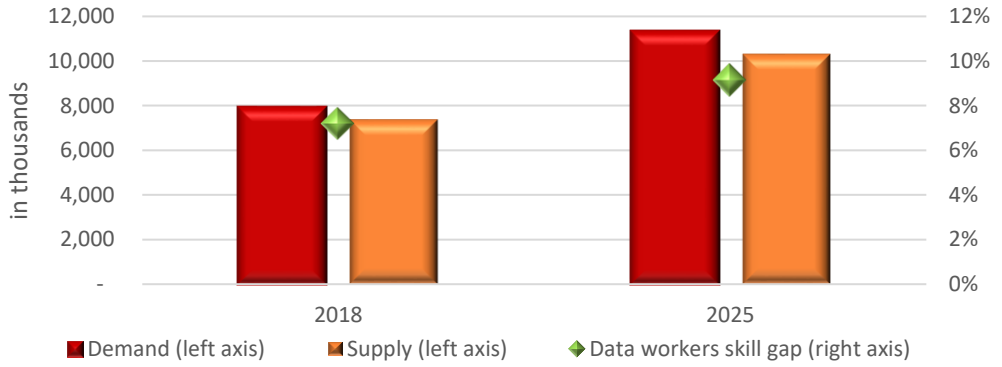
Artificial Intelligence feeds on data to train algorithms, but data-driven companies are struggling to find skilled personnel. From data collection to data transfer, storage and analytics, human capital is key to the entire value chain. By and large, the problem is finding people with the right mix of skills, i.e. the data scientists, who combine technical skills, analytical and industry knowledge, business sense and soft skills to turn data into value for employers. These people are very hard to

[17] Key Enabling Technologies - micro and nano electronics, nanotechnologies, industrial biotechnologies, advanced materials, photonics and advanced manufacturing.

find. Despite advances in both the perception of data as a strategic resource for companies, and the burgeoning government support for digital skills, the evidence shows that data potential is still not being met. Core analytical skills as well as highly skilled talent is still needed. Skills are a pathway to employability and prosperity. They are a pull factor for investment and a catalyst in the virtuous circle of job creation and growth. However, the skills gap and mismatches are very obvious. 40% of European employers have difficulty finding people with the skills needed to grow and innovate. According to current data and estimates for the future, there is (and there will be) a substantial skills gap. According to IDC, in 2018, the gap between total demand and supply of data workers was 571,000 unfilled data worker positions in the EU (corresponding to 7.2% of total demand) and this is expected to rise to over 1 million (9.2% of total demand) by 2025 (Fig. 5.6). In the scenario to 2025, skills gap in both Germany and France are expected to more than double – from 5% to 11.3% in the former and from 4.8% to 11% in the latter – thus becoming, together with Spain, the countries that will suffer the most from the shortage of necessary data skills (Fig. 5.7). The UK, one of the leading data markets in Europe, is expected to show the lowest gap. Because of the reduction in its economic growth potential due to Brexit, the growth of the demand for data workers is expected to slow down as well by 2025. At the same time, the UK education system will increase its offering. The resulting data skills gap is mid-sized (5.6% in 2025) and lower than the EU average. Poland shows a data skills gap in line with those exhibited by most of the EU Member States. Given its positive growth trend, Poland is expected to reach a high level of data skills demand by 2025 with a corresponding potential risk of gap.

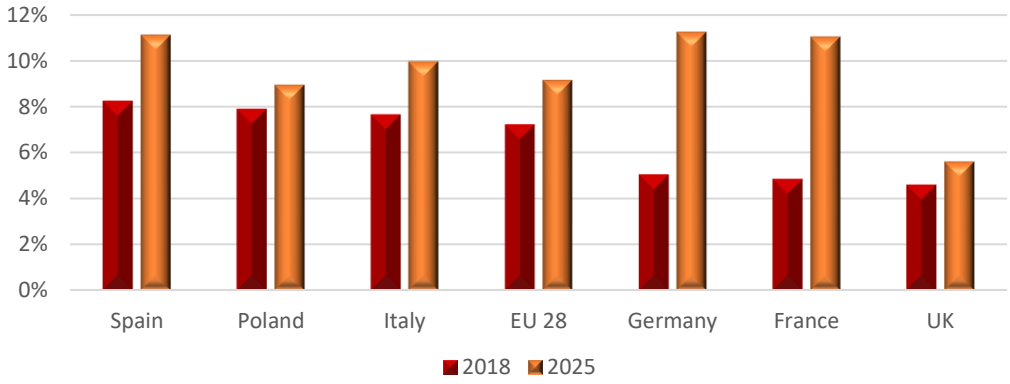
As already stated, AI-linked advances are increasingly transforming the nature of work not only for repetitive tasks but also for the more sophisticated ones in administrative, legal or supervisory areas. While not all jobs will require highly advanced doctorate degrees, they will need varying levels of appropriate skills. These skills are likely to become prerequisites for a number of workers, from chief executive officers to entry-level positions. In terms of the occupational mix, most data workers are professionals, technicians, or associate professionals (70% total) (Fig. 5.8), however, there is also a significant number in the manager category (23%), largely focusing on data in order to drive their decisional processes. Existing managers, at all levels, need to become more familiar with and use data and analytics. On the other hand, only 7% of data workers concerns clerical support roles.

Fig. 5.6: Data worker skills gap



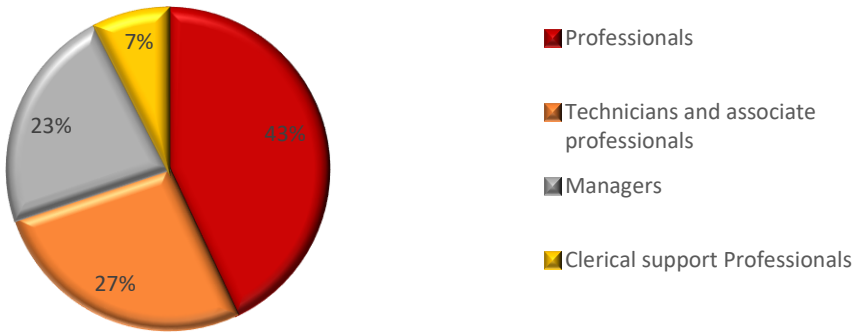
Source: I-Com elaboration on data European Data Market Monitoring Tool, IDC (2019)

Fig. 5.7: Data worker skills gap in the Big Five countries and the EU



Source: I-Com elaboration on data European Data Market Monitoring Tool, IDC (2019)

Fig. 5.8: Occupational Mix of Data Workers (2018)



Source: I-Com elaboration on data European Data Market Monitoring Tool, IDC (2019)

5.3. European initiatives

The spread of digital tools is having a massive impact on the labor market and the type of skills needed in the economy and society. Digitalization is revolutionizing employment, automating "routine" tasks and creating new and different types of jobs in all sectors of the economy.
It is leading to the need for every citizen to have at least basic digital skills in order to live, work, learn and participate in modern society.
Starting in 2013, the Commission initiated the **Grand Coalition for Digital Jobs** as a cross-European, multi-stakeholder initiative to increase the provision of digital skills through stakeholder pledges offering ICT training, apprenticeships, placements, actions to facilitate mobility and/or carrying out awareness raising activities to encourage young people to study and pursue careers in ICT.
On 18 April 2016, the Commission published a **Communication on Digitalizing European Industry**, which introduced a set of coherent policy measures as part of a Digital Single Market (DSM) technologies and public services modernization package, including a specific section (4.4.) on digital skills. It specifically calls for a human capital ready for the digital transformation with the necessary skills.
The purpose of this Communication is therefore to reinforce the EU's competitiveness in digital technologies and to ensure that every industry in Europe, in whichever sector, wherever situated, and no matter of what size, can fully benefit from digital innovations. The document specifically underlines that the digital transformation is structurally changing the labor market and the nature of work imposing the possession of digital skills and the acquisition of other different skill sets.
On 10 June 2016, the Commission adopted the new **Skills Agenda for Europe,** launching 10 actions to make the right training, skills and support available to people in the EU. The Plan aims to help low-skilled adults acquire a minimum level of literacy, numeracy and digital skills and/or acquire a broader set of skills by progressing towards an upper secondary qualification or equivalent, support better understanding of qualifications and make better use of all available skills in the European labor market, improve the digital skills of the wider population, and not just IT professionals.
On 17 January 2018, the Commission launched new measures to boost key digital competences and skills. It involves 3 initiatives: a **Recommendation on Key Competences for Lifelong Learning** (which recommends steps to foster competences in science, technology, engineering and mathematics - STEM - and motivate more young people to embark on a career in these fields); a **Recommendation on Common Values, Inclusive Education and the European Dimension of Teaching**; and a **Communication on the Digital Education Action Plan.** The latter identifies 3 priorities setting out 11 initiatives to help EU Member States to meet the challenges and opportunities of education in the digital age: a) making better use of digital technology for

teaching and learning. This priority is articulated in 3 actions: 1) Connectivity in Schools intending to raise awareness on the benefits of high capacity broadband for schools and to tackle the digital divide between and within EU countries by providing information on financial support from the EU for connectivity and developing a voucher scheme for schools for improved connectivity; b) SELFIE self-reflection tool and mentoring scheme for schools providing the offer to any school in Europe of the possibility of using SELFIE, a free, online self-reflection tool on the use of digital technologies and the launch of a mentoring scheme to scale up ICT-based innovative practice between schools at different stages of technology integration; 3) Digitally Signed Qualifications focusing on the adoption of digitally-signed qualifications able to ensure that certificates from one Member State can be understood and correctly interpreted in any other; b) developing relevant digital competences and skills for the digital transformation through 5 initiatives to create an EU-wide online platform supporting Higher Education institutions (HEIs) in using digital technologies, foster digital competences and open science skills in higher education, encourage more primary, secondary and vocational schools to take part in the EU Code Week, increase awareness of the risks faced when being online and support capacity building of educators in online safety and foresee a series of workshops on digital and entrepreneurial skills for girls in primary and secondary education; and c) improving education through better data analysis and foresight.
The acquisition and strengthening of digital skills is a priority included in several funding programs. As part of the next long-term EU budget - the Multiannual Financial Framework - the Commission has proposed the Digital Europe Program, a program focused on building the strategic digital capacities of the EU and on facilitating the wide deployment of digital technologies, to be used by Europe's citizens and businesses. With a planned overall budget of €9.2 bln, it will shape and support the digital transformation of Europe's society and economy. The program will boost investments in supercomputing, artificial intelligence, cybersecurity, advanced digital skills, ensuring a wide use of digital technologies across the economy and society focusing on 3 types of actions: 1) Master's Programs in cutting-edge digital technologies developed together with EU excellence centers in AI, cyber and high-performance computing (to offer 160 new master programs training 80,000 digital specialists); 2) Short-term specialized training courses in advanced digital technologies for around 150,000 job seekers and employed people especially in SMEs (to equip them with the competences that will enable the deployment of digital technologies across all sectors of the economy); 3) 35,000 job placements in companies or research centers where advanced digital technologies are developed or used (to give people the opportunity to learn specialists' skills working with the latest available technologies); b) the European Social Fund Plus will support EU Member States to improve the quality, effectiveness and the labor market relevance of national education and training systems to support the acquisition of key competences, including digital skills. It will also support upskilling and reskilling opportunities for

all, focusing on digital skills; c) the European Globalization Adjustment Fund supports people losing their jobs as a result of major structural changes in the world through a maximum annual budget of € 150 mln for the period 2014-2020. It can fund up to 60% of the cost of projects designed to help workers made redundant find another job or set up their own business.

6. SMART CONSUMERS IN THE DIGITAL AGE

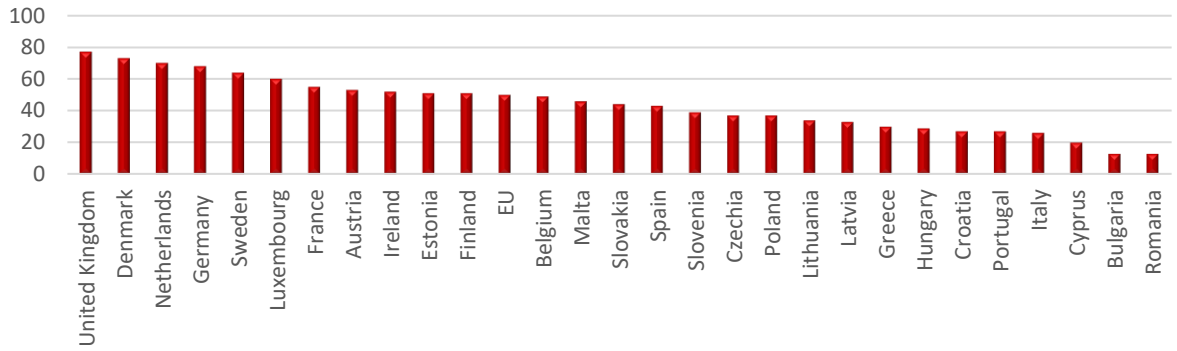
6.1. Smart consumers in the European and international context

The spread of Internet and digital technologies has radically transformed the socio-economic context in which citizens and companies operate. The network has become the epicenter of our life. Nowadays, we use the web to communicate, find information, buy and sell goods or services, interact with public administrations and many other activities that before we had done through traditional channels. One of the most important activities that individuals perform online is the purchase of goods and services. Whereas the retail sector, in general, is still facing difficult times, online shopping is continuing to grow. Among the 10 countries with the highest penetration rates of online sales in mid-2017, we find China and South Korea (83%) at the top, followed by the United Kingdom. E-commerce in Europe is forecasted to be worth € 621 bln by the end of 2019[18]. This would mean an increase of 13.6% compared to the situation last year, when e-commerce was worth € 547 bln. According to Eurostat data, 50% of European citizens made at least one online purchase in the last three months of 2018, with the UK leading (77%), followed by Denmark (73%) and the Netherlands (70%), while Bulgaria and Romania had the lowest percentages (Fig. 6.1).

Furthermore, there appears to be a reverse relationship between age and Internet purchases of individuals (Fig. 6.2). The 25-34year age bracket was more inclined to make purchases online in the EU (67% of individuals making at least one online purchase in the last 3 months of 2018). However, in the Central and Northern European countries the percentage of individuals making at least one online purchase in the last three months of 2018 was high for all age brackets. In the UK and Denmark, the percentage of individuals in the 65 to 74 age brackets buying online was 59%. The worst performers were Bulgaria and Romania with no age brackets exceeding 23%.

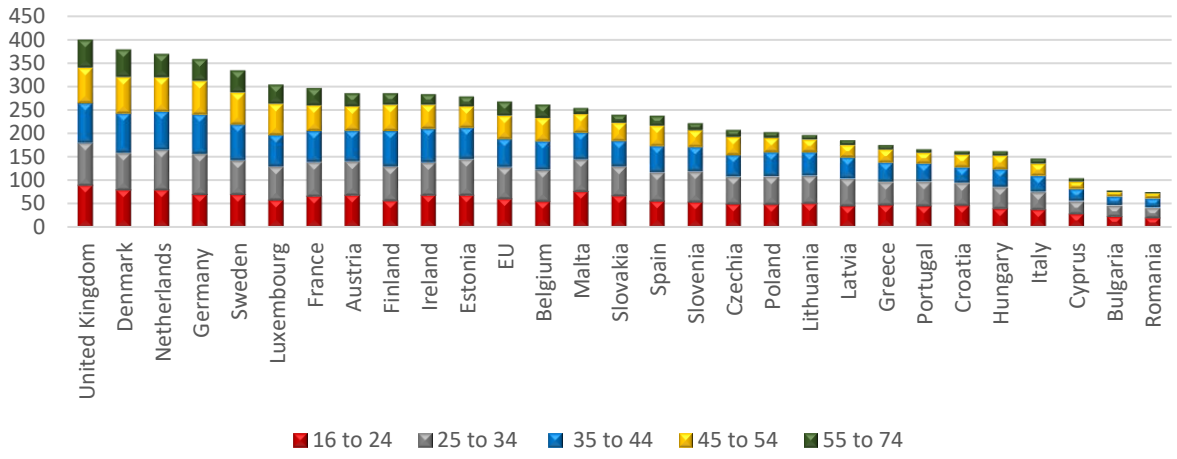
[18] European Ecommerce Report 2019

Fig. 6.1: Internet purchases by individuals in the last 3 months of 2018 (%)



Source: Eurostat

Fig. 6.2: Internet purchases of individuals by age range (%, 2018)

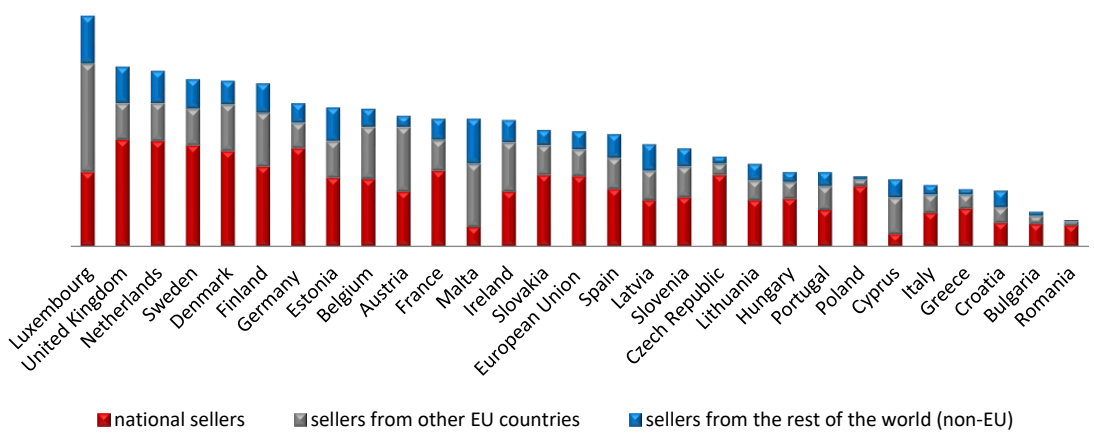


Source: Eurostat

Most individuals in the EU buy online exclusively from national sellers (Fig. 6.3). Considering the importance of e-commerce spreading across Europe, the European Commission tabled a package of measures to allow consumers and companies to buy and sell products and services online more easily and confidently across the EU. The E-commerce Package was made up of legislative proposals to address unjustified geo-blocking and other forms of discrimination on the grounds of nationality,

residence or establishment, to increase pricing transparency and correct regulatory practices and strengthen the enforcement of consumer rights and guidance to clarify, among others, what qualifies as an unfair trading practice in the digital world. In particular, high delivery charges in cross-border deliveries - prices charged by postal operators to deliver a small parcel to another Member State are often up to 5 times higher than domestic prices - prevent consumers and small businesses from selling or buying more across the EU. Therefore, the Commission's proposal was to increase pricing transparency and the regulatory controls of cross-border parcel delivery services.

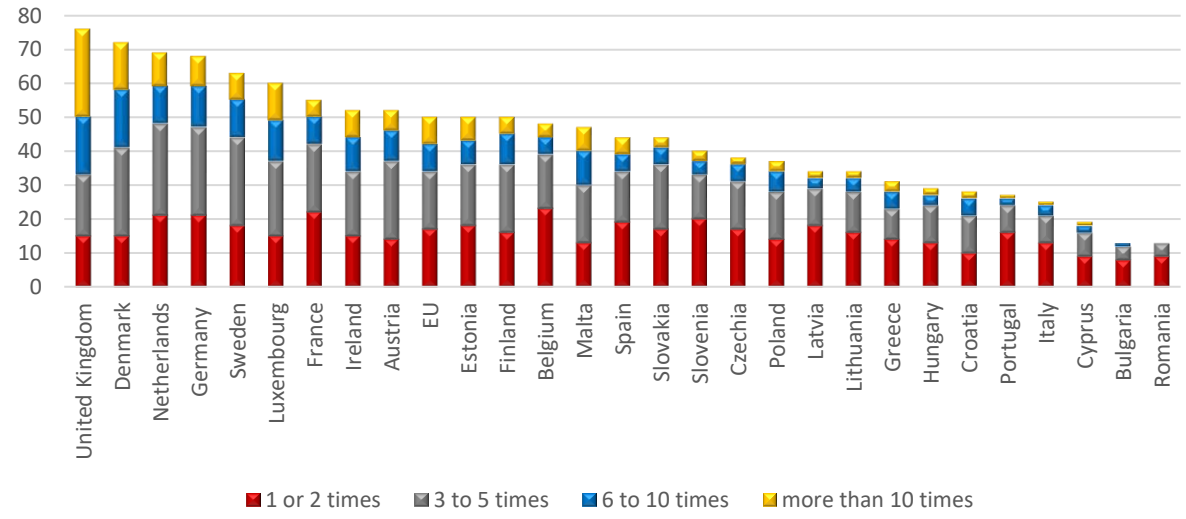
Fig. 6.3: Online purchases - origin of sellers (%, 2017)



Source: Eurostat

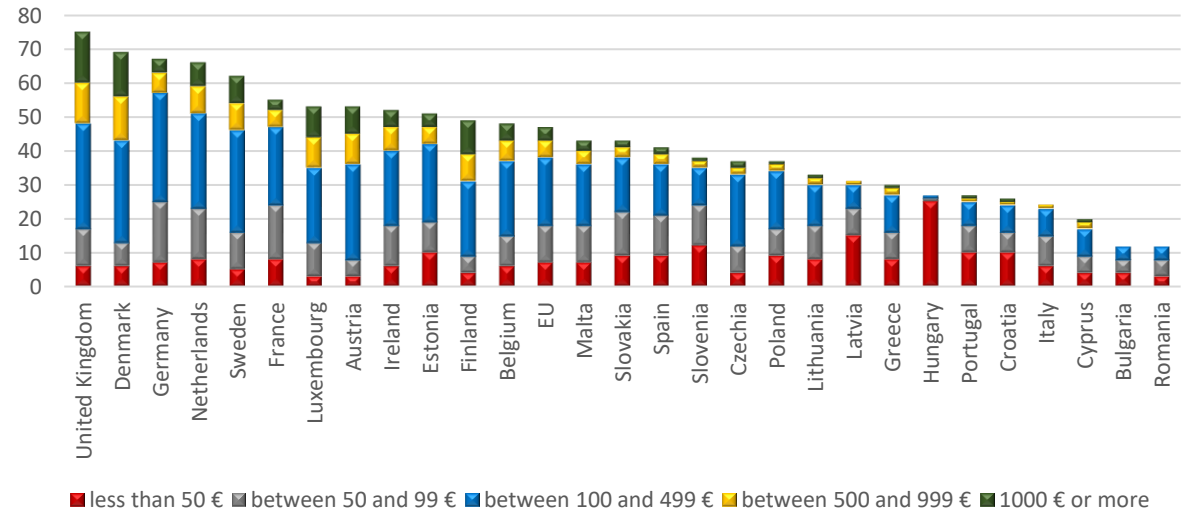
In the last 3 months of 2018, on average, 17% of EU individuals made from 1 to 2 online purchases, 17% from 3 to 5, 8% from 6 to 10 and 8% more than 10. Central and Northern Europeans purchased online more frequently than those in the Southern and Eastern countries. In the UK and Denmark, the percentage of individuals purchasing online more than 10 times in the 3 months was 26% and 14%, respectively (Fig. 6.4). Most online purchases were for a cost ranging from 100 to 499 euros (20%). This means that citizens' trust in digital shopping channels is slowly increasing. With the exception of Hungary (25%), few citizens of European countries decide to buy low-value common goods online. Only 7% of individuals made an Internet purchase of less than 50 euros (Fig. 6.5).

Fig. 6.4: Frequency of online purchases in the last 3 months of 2018 (%)



Source: Eurostat

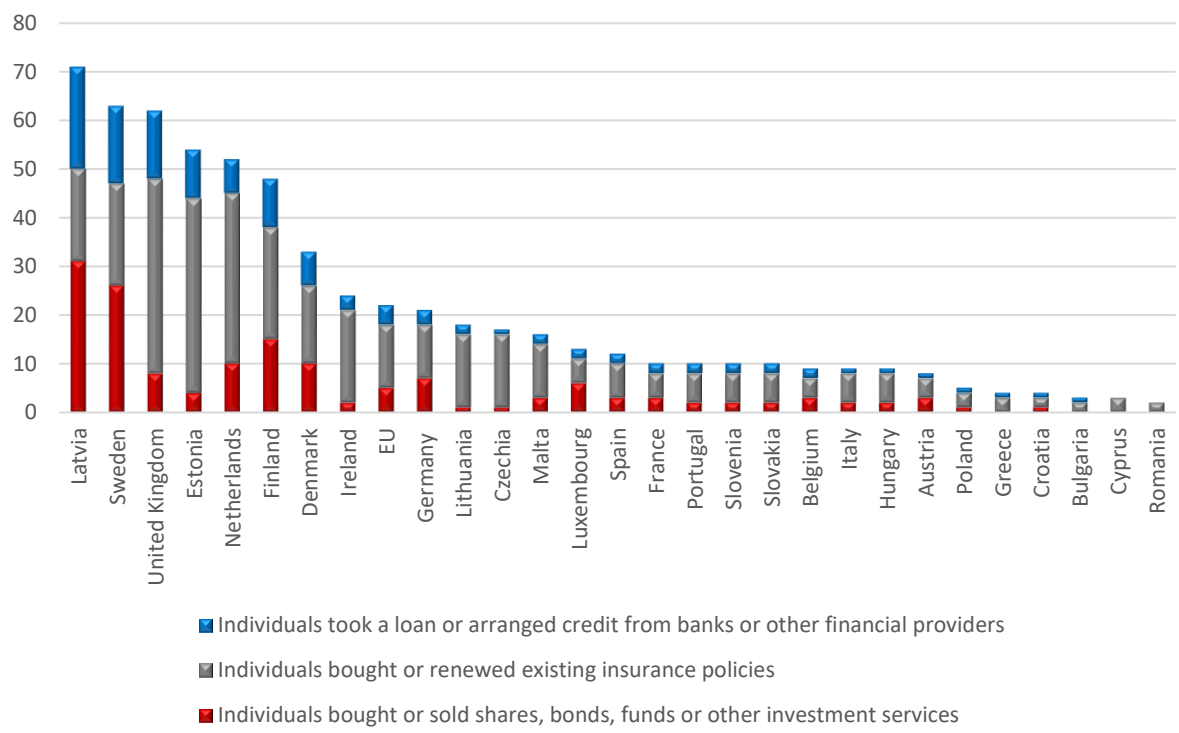
Fig. 6.5: Spending in online purchases in the last 3 months of 2018 (%)



Source: Eurostat

The confirmation of the greater climate of trust of individuals towards digital channels is also evident by observing the number of financial transactions that European consumers have made online in 2018 (Fig. 6.6). Until that year, this type of transaction was carried out exclusively through trusted operators in banks or in insurance. In 2018, 5% of individuals in Europe bought or sold shares, bonds, funds or other investment services over the Internet, 4% took out a loan or arranged credit from banks or other financial providers and 13% bought or renewed existing insurance policies.

Fig. 6.6: Financial activities of individuals over the Internet (%, 2018)



Source: Eurostat

6.2.Consumer protection in the global context

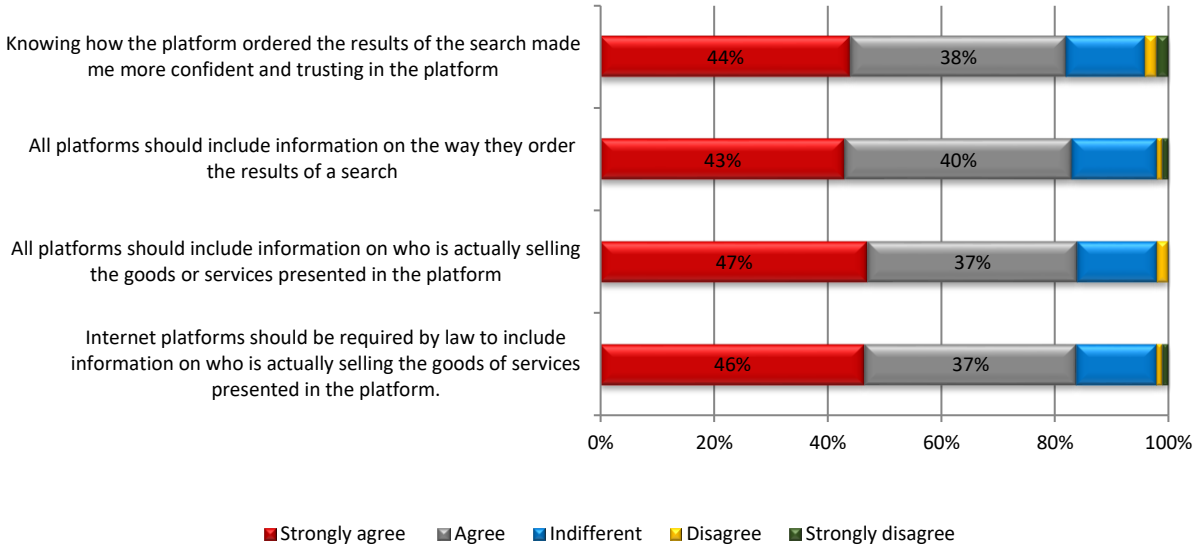
As we saw in the previous chapter, the number and types of applications that individuals perform over the Internet are increasing dramatically. It is therefore necessary to implement new protection systems to ensure that their rights are respected even on digital channels. The success of the Digital Single Market depends especially on the confidence and trust of consumers. Millions of European consumers use online platforms (e.g. search engines, social media, e-commerce platforms, app stores, price comparison websites) to access goods and services and these platforms enable consumers to find online information and businesses to exploit the advantages of e-commerce. Online platforms provide opportunities for innovation and growth in the Digital Single Market, but, at the same time, they could pose significant challenges to consumer protection and market competition. According to the policy paper "Online platforms and how to regulate them: an EU overview" (2018), the concerns over the power of online platforms raised in the ongoing political debate can be roughly grouped into two categories:

1. Competition and market power: platforms generate regulatory concerns because of their expanding market power. Many platform markets tend towards domination by one or very few players, thanks to, among other things, strong network effects and economies of scale advantages. Another concern is the way in which platforms are able to leverage their exclusive access to vast amounts of consumer, business and transactional data. These data troves give them a constantly self-reinforcing knowledge edge concerning market dynamics over competitors and regulators alike.
2. Algorithmic discrimination and information asymmetries: most platforms heavily rely on automated algorithm-based decision-making to process transactions and data. Automated decision-making systems are efficient and often more impartial than human decision makers but they can also perpetuate discrimination and deleteriously affect European citizens. Yet, proving such a discriminatory bias can be complicated: The inner logic of automated decision-making systems remains opaque to businesses and individuals operating on a platform. This so-called "algorithmic black box" also complicates regulatory scrutiny.

According to a survey (2018) published by the EU Commission, included in a study on the transparency of online platforms, about 82% of respondents said that knowing how results were ranked made them more confident and trusting in the platform. Moreover, the great majority of respondents (83%) think that all platforms should include information on the way they order the results of a search as this would make users more confident and trusting in platforms and, in general, would lead to a better service for users. Related to contractual party identification, 84% of those interviewed declared that all platforms should include information about who is actually

selling the goods or services presented in the platform, and around the same percentage agreed that Internet platforms should be required by law to include information about who is actually selling the goods or services on the platform (Fig. 6.7). Furthermore, the majority of respondents agreed that such information would make users more confident and trusting in platforms and, in general, that this would lead to a better service for users.

Fig. 6.7: Results of EU survey on online platforms



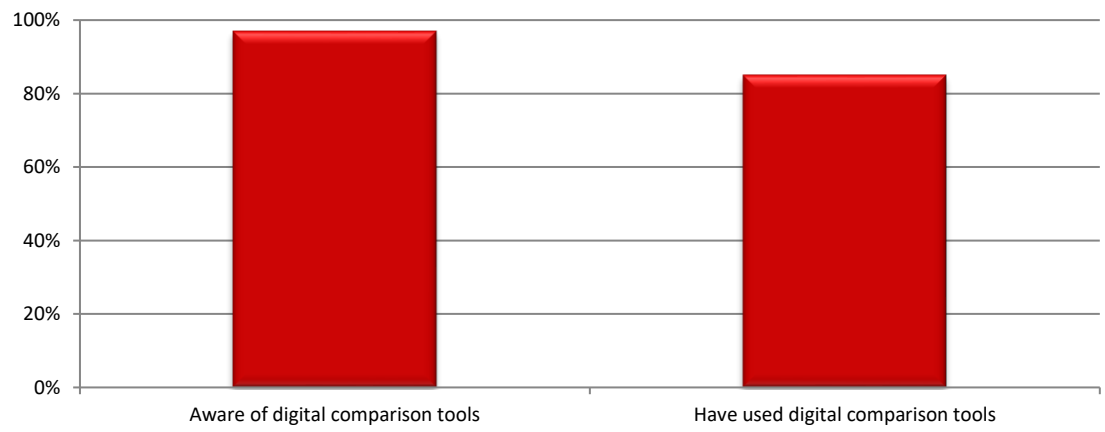
Source: European Commission, 2018

Faced with the growing complex information and choices online, consumers are increasingly using digital comparison tools that guide them in making a decision. Seen as tools of consumer empowerment, price comparison services allow customers to compare product offerings of online sellers, to reveal information on the alternatives and are seen as shifting the traditional asymmetries of information and power between consumers and suppliers.

According to the report, "Digital Comparison Tools Market Study" (2017), published by the Competition and Markets Authority in the United Kingdom, these tools offer two types of benefits. Firstly, they save time and effort in searches and make comparing easier and more appealing, above all for household services that are often complicated and not of immediate interest. Secondly, they make suppliers compete more to provide lower prices and better consumer choices.

In 2010, more than 80% of European consumers used price comparison websites in the travel sector, with five out of ten using them at least once a month. The trend has grown further with the growing use of smartphones and tablets which allow consumers to access and compare information on prices, quality and product specifications in all sectors at any time.
The CMA consumer survey found that 97% of UK consumers were aware of digital comparison tools and 85% of UK consumers with access to the Internet have used online comparison tools at least once before purchasing (Fig. 6.8) and in 2015 it was estimated that consumers made 11 million transactions through comparison tools in four sectors alone.

Fig. 6.8: Proportion of people that know of and have used digital comparison tools in the UK



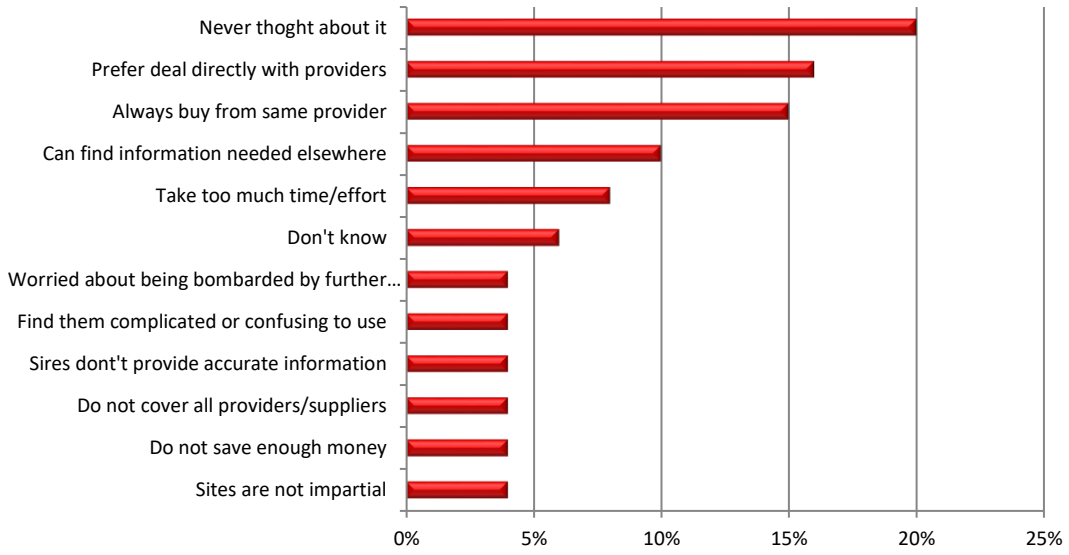
Source: Source: CMA, 2017
Note: The research involved an online survey of over 4,000 consumers and 32 face-to-face interviews with an observational exercise

Online comparison tools do not have unique characteristics as there are many different types of comparison sites on the market that also vary regarding the services offered in different countries (above all for the objective, activities, website operator status, business model and remuneration, comparison method). Some are only limited to comparing information on prices and the main product features while others provide additional services. In general, four types of comparison tool models can be found in Europe:

1. commercial websites run by the private sector
2. commercial websites run by the private sector but certified by the National Authority
3. non-commercial websites run by consumer and/or industry associations
4. non-commercial websites run by public authorities.

Comparison tools can play a positive role in encouraging consumers to go online as they can help identify better deals. Portals equipped with interactive tools for comparing offers are spreading throughout Europe and worldwide, the proof that these tools have become a successful means in many countries. Indeed, also at a European level, the tool for comparing offers is considered a prerequisite for knowledge of the options available on the market and for consumer empowerment, however, there are some consumers who are still not used to these tools. According to the CMA survey, the main reasons consumers had not used a digital comparison tool were a lack of consideration, a preference for alternatives or a range of negative views about comparison sites (Fig. 6.9).

Fig. 6.9: Consumers' reasons for not using comparison sites in the UK

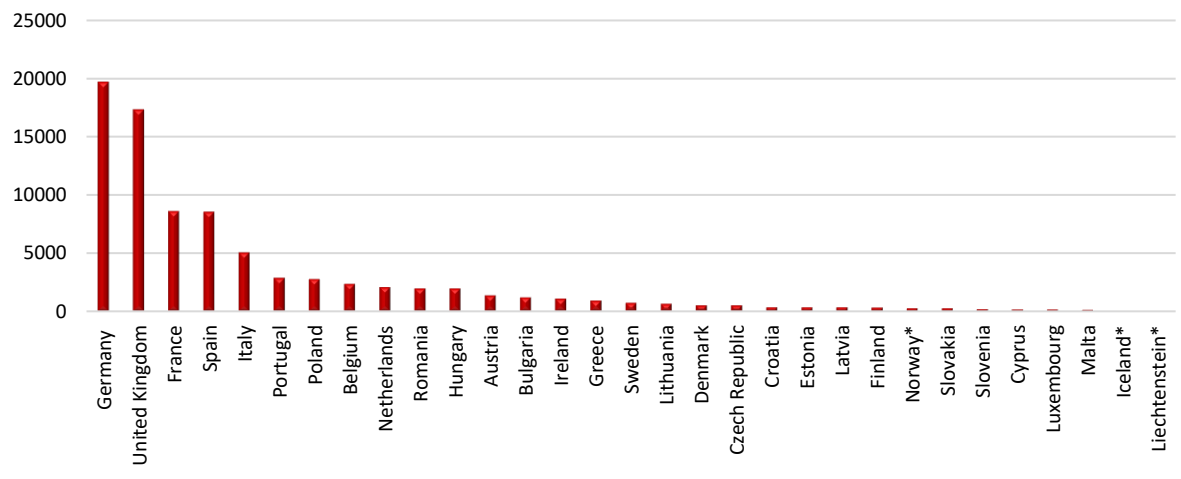


Source: CMA, 2017

Another very useful tool through which consumers can act when they encounter problems in an online purchase is the Online Dispute Resolution. The ODR is a platform provided by the European Commission to allow consumers and traders in the EU or Norway, Iceland and Liechtenstein to resolve disputes relating to online purchases of goods and services without going to court. The ODR platform is not linked to any trader. Using the ODR, the consumer can send the complaint to an approved dispute resolution body (an impartial organization or individual that helps consumers and

traders reach an out-of-court settlement). This is usually quicker and cheaper than going to court. The ODR platform is easy to use and takes users through the dispute resolution process in a step-by-step fashion. It provides translations in all EU languages and has inbuilt time limits for resolving complaints. Using ODR, consumers can get fair outcomes for free or for a very small charge, while traders can avoid costly litigation procedures and maintain good customer relations. To start a complaint, the consumer and trader both have to be based in the EU or Norway, Iceland or Liechtenstein. Once the trader has agreed to use the dispute resolution procedure to address the complaint, the consumer will have 30 days to agree on the dispute resolution body that will handle the dispute. The trader will send to the consumer, through the platform, the name of one or more dispute resolution bodies able to deal with it. Traders are not obliged to engage in the online dispute resolution process, so a trader can refuse to accept your complaint through the ODR platform. Having the ODR link on their website does not automatically mean a trader will engage in the process. Traders based in Belgium, Germany, Luxembourg or Poland can also use the ODR platform to make a complaint against a consumer for a dispute concerning goods and services purchased online. According to data collected by the online dispute resolution platform, approximately 82,000 disputes were submitted up to 17 September 2018. German consumers are those who have opened more disputes on the platform (19,683), followed by the British (17,333), the French (8,597) and the Spaniards (8,548) (Fig. 6.10).

Fig. 6.10: Online Dispute Resolution - Country of consumer



Source: Online Dispute Resolution (https://ec.europa.eu/consumers/odr/main/?event=main.statistics.show)
Note: * non-EU countries / data extracted on 17-09-2018

6.3. EU consumer policies

Analyzing the European regulation on consumers, several different areas can be identified. Referring to the other chapters and the analysis of the specific initiatives launched on AI, telecommunications networks, data protection and the labor market, this section will briefly describe some of the most important actions impacting consumers, subdivided by subject.

Shopping and e-commerce

Shopping is one of the most important areas to be analyzed, considering the opportunities and also the specific critical issues arising from the digital market. In fact, the first pillar of the Digital Single Market Strategy specifically includes initiatives to encourage the development of e-commerce.

The Commission has launched several initiatives regarding this. The Communication *"A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses"* (25.05.2016) presented a package of measures containing four key DSM proposals to boost the potential for cross-border e-commerce in Europe. They are: 1) a legislative proposal on addressing unjustified **geo-blocking** and other forms of discrimination based on nationality, place of residence or place of establishment within the Single Market; 2) a legislative proposal revising the Regulation on **Consumer Protection Cooperation**; 3) a legislative proposal (Regulation) proposing measures in the area of **parcel delivery**; and 4) a guidance on the implementation/application of the Directive on **Unfair Trading Practices**.

Postponing the analysis of the legislative proposal revising the Regulation on Consumer Protection Cooperation and guidance on the implementation/application of the Directive on Unfair Trading Practices to the paragraph on consumer protection, on **28 February 2018**, the **Regulation (EU) 2018/302 addressing unjustified geo-blocking and other forms of discrimination based on a customer's nationality, place of residence or place of establishment within the internal market,** and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC, was adopted (taking effect from 3 December 2018). It was aimed at preventing discrimination on the above in cross-border transactions between a trader and a customer relating to the sales of goods and the provision of services within the Union. To achieve these goals, the regulation prohibits traders to block or limit, through the use of technological measures or otherwise, a customer's access to the trader's online interface for reasons related to the customer's nationality, place of residence or place of establishment.

To contribute to fostering growth through the creation of a true Digital Single Market, after the presentation, on **9 December 2015**, of a **proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content,** on **20 May 2019,** the Directive 2019/770 was adopted. It is a very important measure that declines for digital content or services the most important protection tools provided for consumers by traditional

regulatory frameworks. To this end, it regulates any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price, and also when the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader (except where the personal data provided by the consumer is exclusively processed by the trader for the purpose of supplying the digital content or digital service).

The Directive establishes the liability of the trader for any failure to supply the digital content or digital service or a lack of conformity and places on the trader a specific burden of proof (art. 12). The same directive regulates the remedies for the failure to supply, attributing the consumer with the right to terminate the contract, and defines remedies for lack of conformity, providing the right of consumer to have the digital content or digital service brought into conformity, unless this would be impossible or would impose costs on the trader that would be disproportionate, taking into account all the circumstances of the case. Art. 14 attributes the consumer with the right to obtain a proportionate reduction in the price or the termination of the contract. The following art. 15-17 sets the rules on the exercise of the right of termination and the obligations of the trader and of the consumer in the event of termination. The same directive also fixes the terms of reimbursement by the trader (14 days from the date on which the trader is informed), in the case of the consumer exercising the right to obtain a price reduction or to terminate the contract and, considering the complexity of the digital operations, the right of consumer redress to the liable trader because of any failure to supply the digital content or digital service, referring to the national law the identification of the person against whom the trader may pursue recourse.

On the same data (20 May 2019), another proposal launched by the Commission on 9 December 2015 was approved - Directive 2019/771 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC. This directive lays down certain requirements concerning distance sales contracts concluded between the seller and the consumer (with the exclusion of contracts for the supply of digital content or digital services), setting rules on conformity of goods, remedies in case of non-conformity and the modalities for the exercising of those remedies.

Concerning measures in the area of parcel delivery, Regulation (EU) 2018/644 on cross-border parcel delivery services was adopted on 18 April 2018, entering into force on 22 May 2018. It considers that the tariffs applicable to cross-border parcels and other postal items for low volume senders, particularly for SMEs and individuals, are still relatively high with a direct negative impact on users seeking cross-border parcel delivery services, especially in the context of e-commerce. Art. 1 identifies the subject matter and objectives concerning: a) regulatory controls for parcel delivery services; b) transparency of tariffs, and assessment of tariffs for certain cross-border

parcel delivery services for the purpose of identifying those that are unreasonably high; and c) information for consumers made available by traders concerning cross-border parcel delivery services.

Consumer protection

Consumer protection is one of the most ambitious goals of the European Commission which has launched different initiatives over the years.

Regulation (EC) 2006/2004 on Consumer Protection Cooperation (the CPC Regulation) lays down a cooperation framework enabling national authorities from all countries in the EEA to jointly address breaches of Union laws protecting consumer interests in cases where the trader and the consumer are based in different countries. The CPC Regulation links national competent authorities to form a European enforcement network called the "CPC Network". In each country, a single liaison office is responsible for coordinating the relevant national authorities which cooperate on consumer rules on unfair trading practices, e-commerce, comparative advertising, package holidays, online selling and passenger rights.

On 25 May 2016, to improve the existing mechanism for cooperation between national consumer protection cooperation authorities, the Commission put forward a proposal for the reform of the Consumer Protection Cooperation Regulation and the replacing of the CPC Regulation by a new regulation.

After successful negotiations among the co-legislators, the new CPC Regulation (**Regulation (EU) 2017/2394**) was finally adopted and published in the EU Official Journal on 27 December 2017.The Regulation entered into force on 17 January 2018, being applicable from 17 January 2020.

This Regulation sets out a number of improvements that will enable EU consumer protection laws to be better enforced. It provides enforcement authorities with additional powers, setting minimum powers for the competent authorities, that are investigation and enforcement powers and also identifies the exercise of minimum powers.

In 2017, the European Commission carried out a thorough analysis of existing regulations which showed that the current EU rules were not being applied and enforced effectively across all countries. Therefore, on 11 April 2018, the European Commission launched a **New Deal for Consumers** to ensure that all European consumers fully benefit from their rights under Union law. The New Deal would empower qualified entities to submit representative actions on behalf of consumers, introduce stronger sanctioning powers for Member State consumer authorities and also extend consumer protection. The Commission Communication identifies several aims: 1) to modernize existing rules and fill the gaps in the current consumer acquis; 2) to provide better redress opportunities for consumers, support effective enforcement and greater cooperation of public authorities; 3) to increase cooperation with partner countries outside the EU; 4) to ensure equal treatment of consumers in the Single Market and guarantee that national competent

authorities are empowered to tackle any problems with 'dual quality' of consumer products; 5) to raise the awareness and strengthen the capacity-building of consumers and traders; and 6) to look at future challenges for consumer policy in a fast evolving economic and technological environment.

To achieve the above, this Communication is accompanied by two different proposals, presently ongoing. The first, to amend the Council Directive on unfair terms in consumer contracts, the Directive on Consumer Protection in the indication of the prices of products offered to consumers, the Directive concerning unfair business-to-consumer trading practices and the Directive on Consumer Rights, to ensure better enforcement and to modernize EU consumer protection rules, particularly in light of digital developments. The second concerns representative actions for the protection of the collective interests of consumers and repealing the Injunctions Directive 2009/22/EC aimed at improving tools for stopping illegal practices and facilitating redress for consumers where many of them are victims of the same infringement of their rights in mass harm situations.

The first proposal aims to amend four EU Directives that protect the economic interests of consumers. Most of the amendments concern the Unfair Commercial Practices Directive 2005/29/EC1 and the Consumer Rights Directive 2011/83/EU2. For the other two Directives – the Unfair Contract Terms Directive 93/13/EEC3 and the Price Indication Directive 98/6/EC4 – only the penalties are amended to ensure greater harmonization and a more consistent application of the rules. Specifically, the proposal prescribes that the penalties provided by Member States (to be communicated to the Commission) must be effective, proportionate and dissuasive and sets out general criteria to be observed by the administrative authorities or courts. This involves the nature, gravity and duration or temporal effects of the infringement, the number of consumers affected, including those in other Member States, any action taken by the trader to mitigate or remedy the damage suffered by consumers, where appropriate, the intentional or negligent character of the infringement, any previous infringements by the trader, the financial benefits gained or losses avoided by the trader due to the infringement and any other aggravating or mitigating factor applicable to the circumstances of the case. In the event of the imposition of a fine, annual turnover and net profits must be taken into account in the determination of the amount (the maximum amount is at least 4% of the trader's annual turnover in the Member State or Member States concerned).

The second proposal introduces a representative action to ensure an effective and efficient protection of the collective interests of consumers and overcomes the obstacles faced by consumers within individual actions (such as uncertainty regarding their rights and available procedural mechanisms, psychological reluctance to take action and the negative balance of the

expected costs and benefits of individual action). The procedure for the adoption of these proposals is ongoing.

Copyright and Sat-cab Directive

The legislation in force is still Directive 2001/29/EC, with subsequent enforcement (Directive 2004/48/EC on the enforcement of intellectual property rights) and modifications such as on rental and lending rights (Directive 2006/115/EC), on the legal protection of computer programs (Directive 2009/24/EC), on certain permitted uses of orphan works (Directive 2012/28/EU), and on collective management of copyright and related rights and multi-territorial licensing in online musical works ("CRM" Directive 2014/26/EU). Moreover, on 1 October 2018, the EU ratified the Marrakesh Treaty, effectively becoming a party to it as of 1 January 2019. A Directive and a Regulation were adopted in 2017 for the implementation of the treaty under EU law. The first focuses on certain permitted uses of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are visually impaired or otherwise print-disabled (September 2017). The regulation, instead, focuses on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject matter protected by copyright for the benefit of "print-disabled"[19] persons.

A new Copyright Directive was proposed by the European Commission in September 2016 as part of the Digital Single Market strategy. On 12 September 2018, the European Parliament adopted its negotiating position, focusing on 3 main objectives: 1) increasing cross-border access for citizens to copyright-protected content online; 2) giving wider opportunities to use copyrighted material for education, research, cultural heritage and disability; and 3) stimulating creation of high-quality content by introducing clearer rules for a functioning copyright marketplace.

On 13 February 2019, the European Parliament, the Council and the Commission came to a political agreement on a text that needed to be formally confirmed by the European Parliament and the Council, before the EP elections taking place in May. It was then approved by the European Parliament on 26 March 2019 and endorsed by the Council on 15 April 2019. The Directive was published in the Official Journal of the EU on 17 May 2019.

Another goal of the Digital Single Market strategy was to review the Satellite and Cable Directive (93/83/EEC) by assessing if it should also include broadcasters' online transmissions, and further measures to improve cross-border access to them within Europe.

[19] Regulation on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are visually impaired or otherwise print-disabled (Regulation implementing the Marrakech Treaty in the EU), 13 September 2017.

The new **Sat-Cab Directive** is also part of the copyright package. The proposed regulation of this topic was based on a retrospective evaluation of the existing Directive, a study and a public consultation. Key topics are the application of the country of origin principle to some online transmissions of broadcasting organizations, and the collective management of rights to retransmissions by means equivalent to cable. Another goal is allowing for a wider access to online content, in particular those coming from broadcasters, across Europe. EU institutions reached an agreement on the Sat-Cab Directive last December. Finally, the **Directive 2019/789** laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organizations and retransmissions of television and radio programs, and amending Council Directive 93/83/EEC, was adopted on 17 April 2019.

European Electronic Communications Code

Referring to Chapter 2 on the analysis of the European Electronic Communications Code, focusing on consumer protection, it has been extended to the 'over the top' part of the regulation that today concerns telecom services. The Code identifies 3 types of electronic communication services to be regulated - Internet access services (ISPs), interpersonal communication services (also covers the OCs) and the spreading of signals (as in TV or M2M services). The Ott will have to inform customers about the quality of the service offered, like a telco, and compensation if the service provided does not correspond to that guaranteed. It also introduces the right to keep one's phone number up to one month after termination of the contract and the right to reimbursement of the prepaid credit not used at the time of contract termination, as well as compensation in case of delay or abuse in switching to another operator. BEREC (Body of European Regulators for Electronic Communications) will play a key role in helping European countries implement high-capacity networks and will contribute to the smooth and homogeneous application of the measures envisaged by the Code in Europe. Member States will have two years to adopt the necessary provisions for the transposition of the Directive.

Online platforms and illegal content

The European Commission has drafted various proposals to foster an environment in which online platforms thrive, where consumers are protected whilst competition is enhanced.

The 2016 Communication "Online Platforms and the Digital Single Market - Opportunities and Challenges for Europe" identifies 4 guiding policy principles:

1. a level playing field for comparable digital services
2. ensuring that online platforms behave responsibly to protect core values
3. fostering trust, transparency and ensuring fairness
4. keeping markets open and non-discriminatory to foster a data-driven economy.

Recently, the European Commission has developed other proposals and recommendations to ensure transparency and consumer protection in online platforms.

A Recommendation on measures to tackle illegal content online (March 2018) fosters and underlines the political commitment of the preceding Communication "tackling illegal content online, towards enhanced responsibility of online platforms", adopted in September 2017.

Moreover, in April 2018 the Commission proposed an **EU Regulation on promoting fairness and transparency for business users of online intermediation services trading** that was adopted on 20 June 2019 (**Reg. 2019/1150**), together with the creation of an Observatory on the online platform economy.

It aims to contribute to the proper functioning of the internal market by laying down rules to ensure that business users of online intermediation services and corporate website users in relation to online search engines are granted appropriate transparency, fairness and effective redress possibilities. It will also apply to online intermediation services and online search engines provided, or offered to be provided, to business users and corporate website users, respectively, that have their place of establishment or residence in the Union and that, through those online intermediation services or online search engines, offer goods or services to consumers located in the Union, irrespective of the place of establishment or residence of the providers of those services and irrespective of the law otherwise applicable. The Regulation sets several provisions on terms and conditions, restriction, suspension and termination of online intermediation services with specific communication obligations, on information to be offered about ranking and the main parameters applied, about differentiated treatment and data access. The same regulation imposes on providers of online intermediation services the provision for an internal system for handling the complaints of business users and the designation in their terms and conditions of two or more mediators with which they are willing to engage to attempt to reach an agreement with business users. It also encourages the adoption of codes of conduct by providers of online intermediation services and by organizations and associations representing them.

Universal Service

Directive n. 2002/22/EC on universal service and user rights relating to electronic communication networks and services establishes the rights of end-users and the corresponding obligations of undertakings providing publicly available electronic communication networks and services. It also defines the minimum set of services of specified quality to which all end-users have access, at an affordable price in the light of specific national conditions, without distorting competition.

7. CYBERSECURITY IN THE DIGITAL AGE

7.1. Cybersecurity in the digital age: a global overview

The digital revolution has transformed everyday life. Thanks to the Internet, connecting people across the world has never been as easy as it is today. Moreover, the IoT (Internet of Things) has led to the spread of a mass of smart devices for people and businesses. However, this relatively new way of living (always accessible, everywhere and at every moment) has brought to light many new problems in terms of security, and, specifically, cybersecurity.

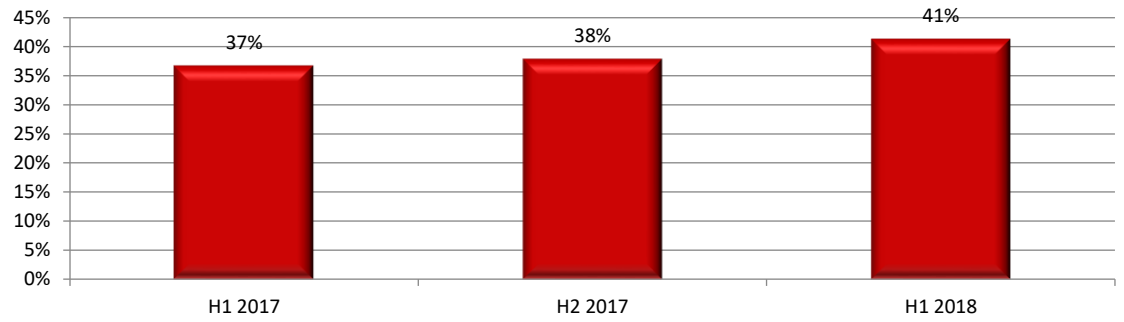
The digital environment is vast and, consequently, it is ideal ground for cyberattacks that can be either indiscriminate or targeted, aimed at large and small organizations in both the public and private sectors. Therefore, Internet usage and its connected devices offer new opportunities for people and 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. The new technologies, mobiles, smart devices connected to the Internet of Things and many artificial intelligence applications expose every organization to attackers, increasing the risks of, for example, shut downs or subversion of industrial control systems. Threats can even be dangerous to human lives if you imagine an attacker being able to turn off life support systems in hospitals or take control of connected cars on the road.

Indeed, the World Economic Forum has included cyberattacks among the biggest problems of 2019, along with natural disasters, biodiversity loss and ecosystem collapse and the spread of infectious diseases[20].

According to the Kaspersky Lab[21], more than 40% of all industrial control system (ICS) computers were attacked by malicious software at least once during the first half of 2018. This is a continuation of a trend with the figure increasing from 36.61% in the first half of 2017 to 37.75% in the second half (Fig. 7.1). Countries with the highest number of ICS computer attacks in 2018 were Vietnam (75.1%), Algeria (71.6%) and Morocco (64.8%). Countries with the lowest number of industrial attacks were Denmark (14%), followed by Ireland (14.4) and Switzerland (15.9%). The largest number of threats come from the Internet, which over the years has become the main source of infection for ICS with 27% of threats being received from the worldwide web, and removable storage media ranking second with 8.4%. Mail clients occupy third place in terms of volume representing 3.8% of threats (Fig. 7.2).

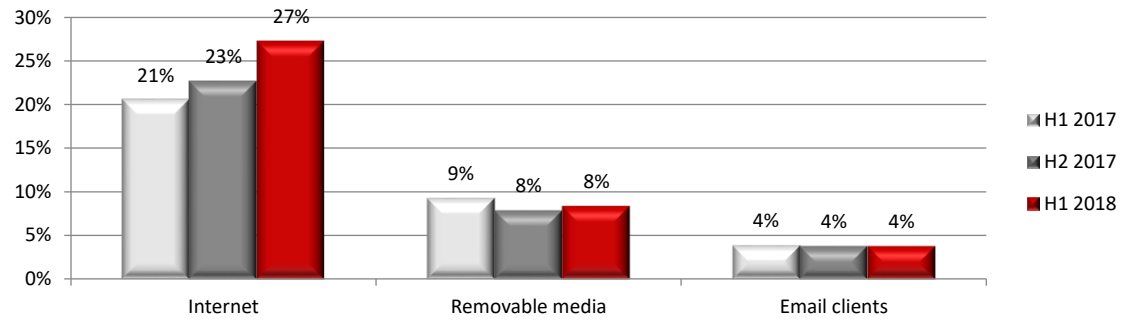
[20] World Economic Forum, "The Global Risks Report", 2019.
[21] https://www.kaspersky.com/about/press-releases/2018_ics-computers-attacked-in-h1

Fig. 7.1: Percentage of industrial control system computers (ICS) attacked



Source: Kaspersky Lab, 2018

Fig. 7.2: Main sources of threats blocked on ICS computers (% computers attacked during half-year periods)

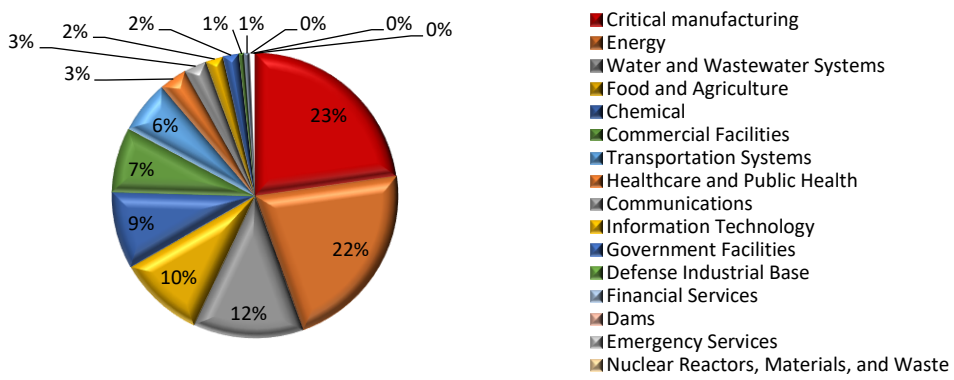


Source: Kaspersky Lab, 2018

The largest number of vulnerabilities affect industrial control systems of manufacturing enterprises (23%), followed by the energy sector (22%) and water supply (12%) companies (Fig. 7.3)[22].

[22] Kaspersky Lab, Threat landscape for industrial automation systems. H2 2018, (2019)

Fig. 7.3: Percentage of vulnerabilities in ICS, by different industries



Source: I-Com elaboration on Kaspersky Lab, 2019

According to a 2019 Clusit study, out of a sample 8,417 serious attacks[23] occurring worldwide between 2011 and 2018, 1,552 were recorded during the last year (+77.8% compared to 2014 and +37.7% compared to 2017) (Fig. 7.4). In recent years, Cybercrime, Cyber Espionage and Information Warfare have recorded a strong increase. Cybercrime rose by 43.8% in 2018 compared to 2017, while Cyber Espionage and Information Warfare increased by 35.6% in 2018 compared to 2017. On the contrary, Hacktivism decreased by -22.8% in 2018 compared to 2017.

Cybercrime is the first cause of serious cyberattacks at a global level. It has gradually been increasing, from 60% of analyzed cases in 2014 to 79% in 2018, showing an unequivocal trend. Hacktivist attacks have progressively decreased, from 27% in 2014 to 4% in 2018. Instead, Cyber Espionage and Information Warfare grew from 13% of total attacks in 2014 to 17% in 2018 (Fig. 7.5).

In 2018, the most affected categories were Multiple Targets (304 attacks, +36.9% compared to 2017), governments (252 attacks, +40.8%) and health (159 attacks, +98.8%).

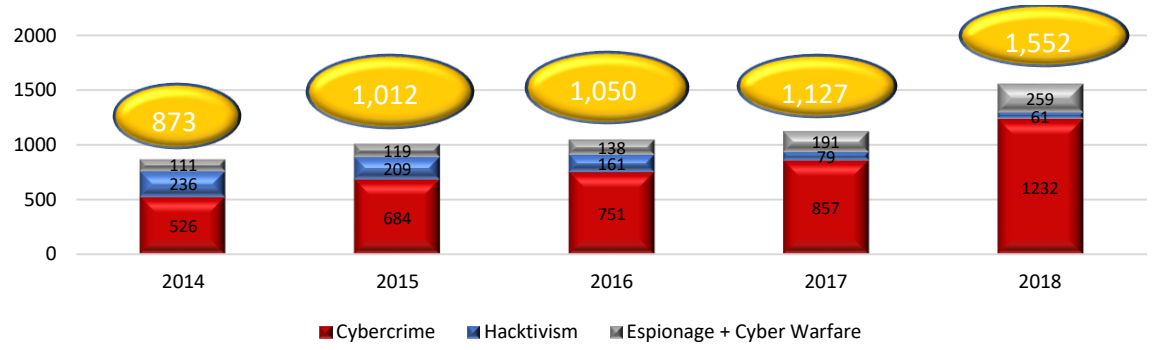
Currently, malware is the most widespread technique of attack. According to McAfee[24], in the first quarter of 2019, ransomware attacks grew by 118%, new ransomware families were detected, and cyber criminals used innovative techniques such as Anatova, designed to cipher all files before requesting payment from the victim.

[23] Serious attacks are those attacks with a significant impact on victims in terms of economic losses, damage to reputation, the dissemination of sensitive personal and non-personal data, or that herald particularly worrying scenarios.

[24] McAfee Labs Threats Report, August 2019

Therefore, in an increasingly digitalized world, cybersecurity has jumped to the top of the company risk agenda after a number of high-profile data breaches, ransom demands, Distributed Denial of Service (DDoS) attacks and others over the last years.

Fig. 7.4: Cyberattacks occurring worldwide (2014-2018)



Source: Clusit, 2019

Fig. 7.5: Distribution of the causes of cyberattacks (2014 Vs 2018)

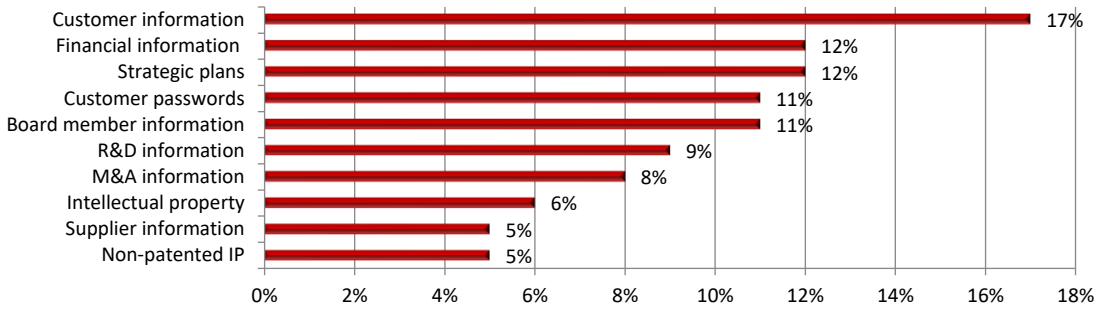
Source: Clusit, 2019

Organizations are spending more on cybersecurity, allocating more resources to improving their defenses, and working harder to embed security-by-design. However, according to the EY Global

Information Security Survey 2018-19[25], more than three-quarters (87%) of organizations do not yet have a sufficient budget to provide the levels of cybersecurity and resilience they require. Protection is patchy, and relatively few organizations are prioritizing advanced capabilities with, too often, cybersecurity remaining siloed or isolated. 39% of organizations said that less than 2% of their total IT headcount work solely in cybersecurity, however, cybersecurity budgets are on the rise.

Customer information, financial information and strategic plans make up the top three most valuable information areas that organizations would like to protect. In fact, for 17% of the organizations interviewed, the biggest fear is the loss of customer information, followed by the loss of financial information (12%) and strategic plan violations (12%) (Fig. 7.6).

Fig. 7.6: Top 10 most valuable information to cyber criminals



Source: EY Global Information Security Survey 2018-19

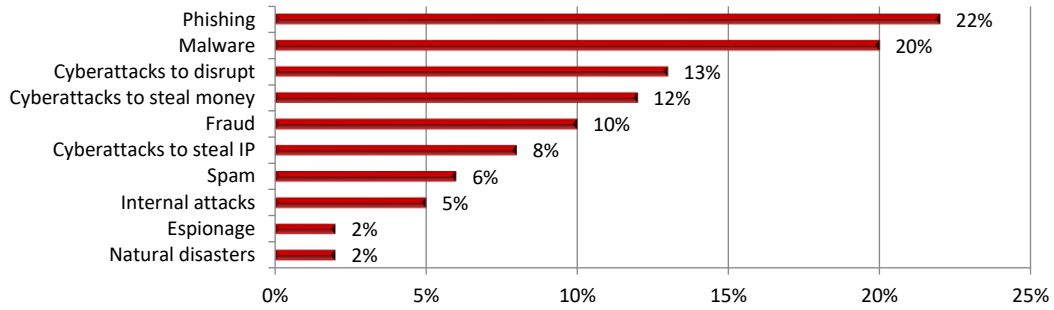
Moreover, 22% of organizations see phishing as the biggest threat, followed by malware (20%) and cyberattacks to disrupt (13%) and to steal money (12%) (Fig 7.7).

Attackers frequently use very simple tools and tactics, such as emails, heavily impacting and damaging companies. Nowadays, emails are not only a communication tool but also one of the prime sources of threat for users and organizations. This threat can range from unwanted emails in the form of spam to more dangerous types, such as the propagation of ransomware or targeted spear-phishing campaigns. According to the Internet Security Threat Report 2019 published by Symantec, some industry sectors receive more spam than others. The spam rate varied from 52.6% for Wholesale Trade to 58.3% for the mining sector. A growing proportion of spam now contains

[25] The 21st edition of EY Global Information Security Survey captures the responses of over 1,400 C-suite leaders and information security and IT executives/managers, representing many of the world's largest and most recognized global organizations.

malware. In 2018, agriculture, forestry and fishing, together with the retail trade, were the sectors most hit by email containing malware. In these sectors, the percentage of email classified as malware made up 11% of total emails. As regards phishing, the trend dropped from 1 in 2,995 emails in 2017, to 1 in 3,207 in 2018 with agriculture being the most affected sector in 2018.

Fig. 7.7: Top 10 biggest cyber threats to organizations



Source: EY Global Information Security Survey 2018-19

Cyberattacks are having a significant and growing financial impact on businesses worldwide. According to the Cost of Cyber Crime Study published by Accenture and the Ponemon Institute (2019)[26], the global average cost of cybercrime, which includes the total of costs incurred to detect, recover, investigate and manage the response to cyberattacks, climbed to $13 mln in 2018, with an increase of 12% from $11.7 mln reported in 2017, and 72% in the last five years (Fig. 7.8).

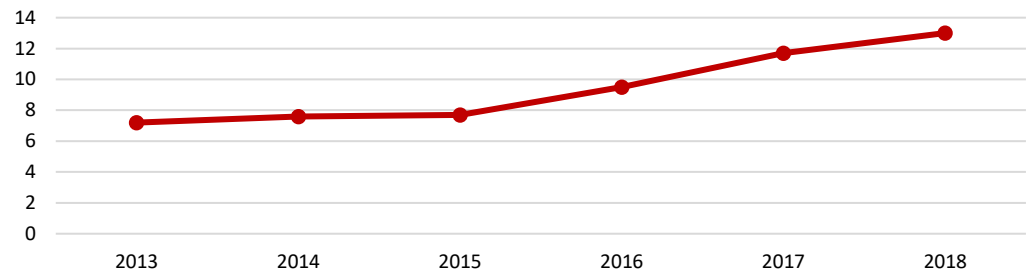
Malware is the most expensive attack type for organizations, followed by web-based attacks, however, the cost of ransomware and malicious insider attack types has grown the fastest over the last year (21% and 15%, respectively).

Analyses show that banking and utilities industries continue to incur the highest costs for cybercrime, equal to $18.37 mln and $17.84 mln with an increase of 11% and 18%, respectively. In comparing different countries, US companies incurred the highest total average cost at $27.4 mln, increasing by 29% in 2018 compared to 2017. But the highest increase of 31% was experienced by organizations in the United Kingdom growing to $11.5 mln, closely followed by Japan increasing by 30% in 2018, reaching $13.6 mln on average for each organization (Fig. 7.9).

Finally, the main and most costly impacts on organizations that suffered cyberattacks are loss of information, business disruption, loss of revenue and damage to equipment.

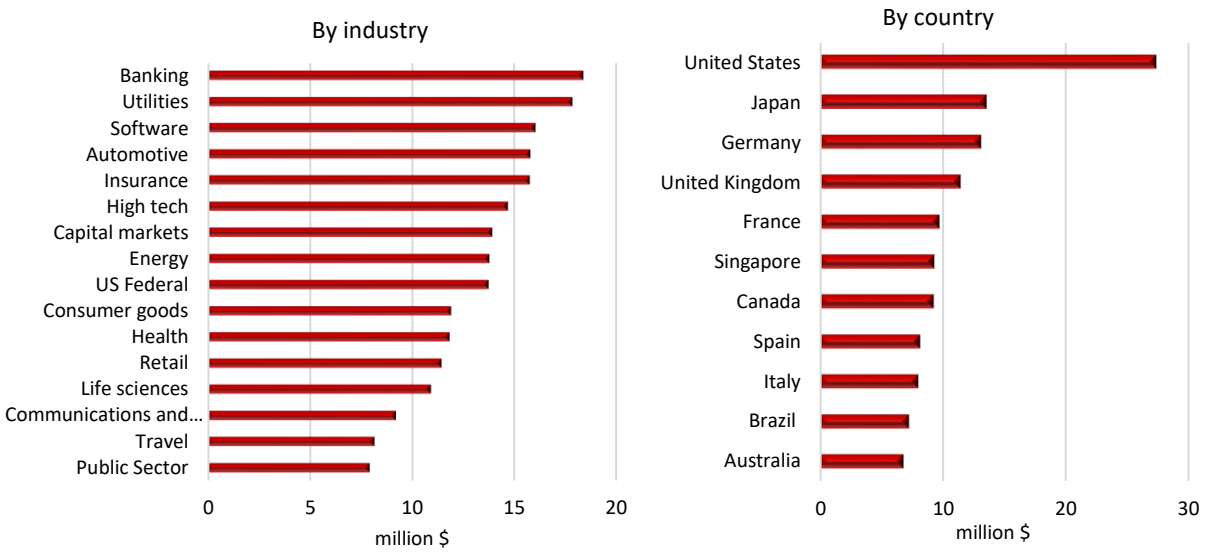
[26] The Cost of Cyber Crime Study surveyed 2,647 security and IT professionals in 355 companies in 11 countries - Australia, Brazil, Canada, France, Germany, Italy, Japan, Singapore, Spain, the United Kingdom and the United States.

Fig. 7.8: The global average cost of cybercrime (million $)



Source: Accenture and the Ponemon Institute, 2019

Fig. 7.9: Cost of cybercrime (2018)



Source: Accenture and Ponemon Institute, 2019

7.2. Experience and awareness of cybersecurity in Europe

Europeans feel increasingly exposed to the risk of falling victim to cybercrime. According to a 2017 Eurostat survey[27], 87% of respondents saw cybercrime as an important challenge to EU security. Over half (56%) saw it as a very important problem, while just under a third (31%) viewed it as a fairly important problem. There are significant country-level differences in the number of respondents who think that cybercrime is a very important security issue, ranging from 76% in Cyprus, and 75% in the Netherlands to only 39% in Sweden and 26% in Estonia.

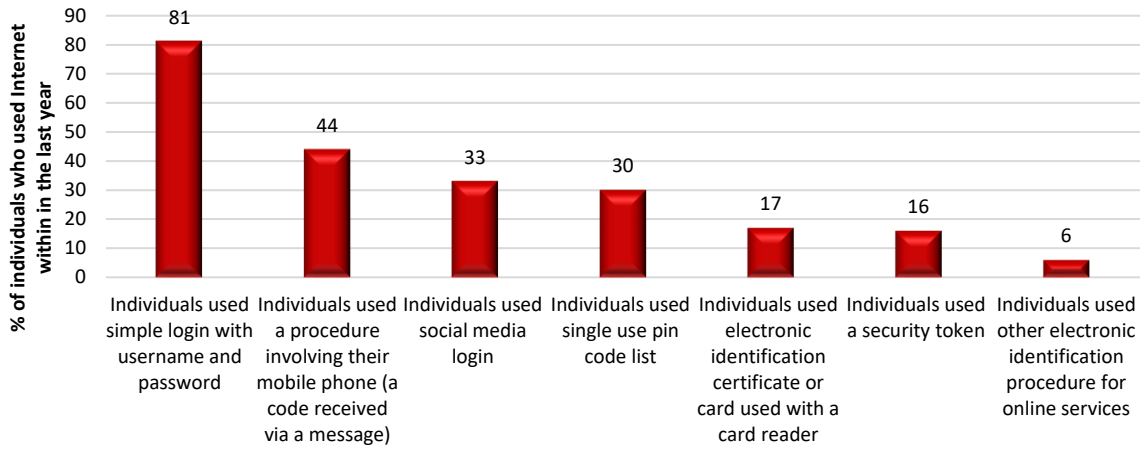
Moreover, Europeans are most worried about the potential misuse of their personal data and the security of online payments. In 2017, 45% of people interviewed by Eurostat were concerned about the possibility that their data might be misused by a third party, while 42% were concerned about the security of online payments.

For this reason, a lot of Internet users in European countries use identification procedures for online services. The use of the tools to ensure secure access to online services and to carry out electronic transactions in a safer way is growing rapidly.

According to Eurostat data, in 2018, over 80% of Internet users in the European Union logged onto online services using their username and password. Other popular identification procedures were by receiving a code by text message on their mobile phone, which was used by 44% of the EU's Internet users. Using social media logins to access other online services (33%) and logging in with a single-use PIN code list (30%) were also popular (Fig. 7.10)

[27] Special Eurobarometer 464°, Europeans' attitudes towards cyber security, 2017.

Fig. 7.10: Identification procedures used for online services in the EU (2018)

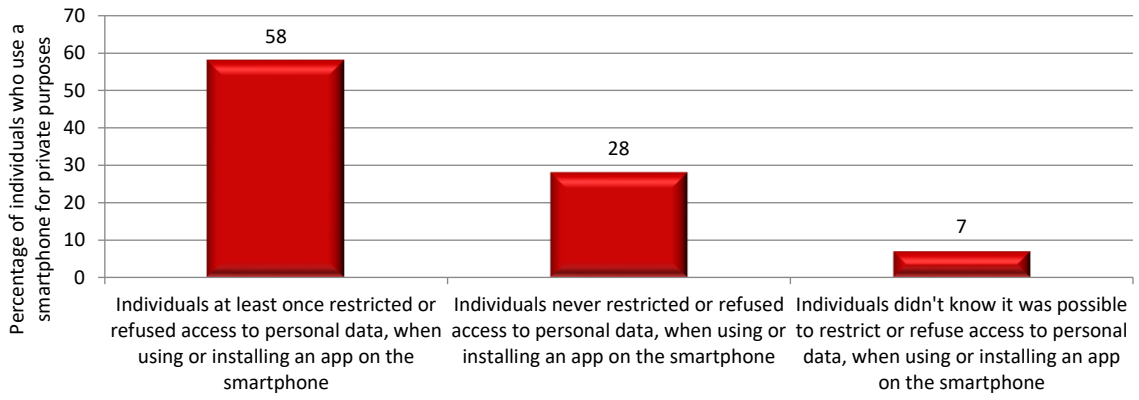


Source: Eurostat, 2019

For example, text messages with a code are a powerful tool in verifying the identity of individuals. In the EU, most Internet users in the Czech Republic (75%), the Netherlands (72%), the United Kingdom (61%) and Denmark (60%) logged in to online services using a procedure involving their mobile phone where a code is received through a text message. In contrast, the lowest percentage for this type of login procedure were recorded in Croatia (4%), Bulgaria and Romania (both 5%)[28]. Use of smartphones to access the Internet has significantly increased and consequently many users are experiencing some security issues, such as viruses affecting devices, abuse of personal information, financial losses, and, therefore, they try to restrict access to their data. According to Eurostat data, in 2018, 58% of individuals at least once have restricted or refused access to personal data, when using or installing an app on their smartphone, while 28% have never restricted or refused access to personal data. Moreover, 7% of individuals did not know it was possible to restrict or refuse access to personal data, when using or installing an app on their smartphone (Fig. 7.11).

[28] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20190205-1

Fig. 7.11: Security and privacy in the use of smartphones in the EU (2018)



Source: Eurostat, 2019

Europe is playing an increasingly active role in addressing the multiple cyber threats and holds a leading position in the global context.

According to the Global Cybersecurity Index 2018 (a composite index combining 25 indicators into one benchmark to monitor and compare the level of the cybersecurity commitment of Member States for the five pillars[29] of the Global Cybersecurity Agenda) published by the International Telecommunication Union (ITU), the UN Agency that deals with TLC and network policies, European countries have improved their rankings due to initiatives such as the EU certification framework for ICT security products, the implementation of the General Data Protection Regulation (GDPR) and the Directive on security of network and information systems (NIS Directive). In 2018, six European countries with the highest level of commitment to cybersecurity were in the top ten most committed countries globally. The United Kingdom dominated the global ranking, followed by France in third position, Lithuania (4th), Estonia (5th), Spain (7th) and Norway (9th).

The United Kingdom ranked first with the highest score in the legal pillar and the organizational pillar, with a number of legal tools to fight cybercrime, including the Computer Misuse Act.

[29] The five pillars are: 1. Legal Measures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime; 2. Technical Measures based on the existence of technical institutions and frameworks dealing with cybersecurity; 3. Organizational Measures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level; 4. Capacity-building Measures based on the existence of research and development, education and training programs, certified professionals and public sector agencies fostering capacity building; 5. Cooperation Measures based on the existence of partnerships, cooperative frameworks and information sharing networks.

France, in third place globally, for the second time running, was ranked in second place in Europe, scoring 100 per cent in the legal and organizational pillars. France is collaborating with institutional partners (ministries, national authorities, private sector and non-profit organizations) and, under the European Cybersecurity Month, is using various means to raise cybersecurity awareness.
Lithuania has the highest score in both the legal pillar and the organizational pillar. The Lithuanian Law on Cybersecurity lays down provisions enabling competent authorities to take action against public electronic communication infrastructures participating in malicious online activity (e.g. participating in a botnet). The State Data Protection Inspectorate can publish cybersecurity incidents involving personal data breaches.
Finally, Europe stands out as having the highest number of Member States with national strategies with, out of a total of 45 European states, as many as 39 having a National Cybersecurity Strategy.

7.3. The European Regulatory Framework

The development of digital services is strongly influenced by the provision of a regulatory framework able to guarantee high levels of security. Cybersecurity is one of the most important priorities for European institutions. In fact, since the adoption of the EU Cybersecurity Strategy in 2013, the European Commission has planned actions to better protect Europeans online. After the adoption of the **EU Cybersecurity Strategy** in 2013 and the **European Agenda on Security** in 2015, on July 6, 2016, the **Directive 2016/1148** (c.d. **NIS Directive**) was adopted, setting measures for a common high-level security for networks and information systems in the Union. The Directive recognizes that network and information system security is essential for economic and social activities and, above all, for the functioning of the Internal market, so to this end, it: 1) has prescribed Member States to adopt a national strategy on network security and information systems; 2) has established a cooperation group to support and facilitate strategic cooperation and information exchanges among Member States and to build trust among them - this group is made up of representatives from the Member States, the Commission and ENISA and carries out its activities on the basis of two-year work programs; 3) creates a network of cybersecurity action teams in the event of an accident to contribute to the development of trust among Member States and to promote rapid and effective operational cooperation; 4) establishes security and notification obligations for operators of essential services and for digital service providers; 5) obliges Member States to identify competent national authorities, single contact points and CSIRTs with tasks related to network security and information systems.
The national strategy must regulate several aspects, in particular, the objectives and priorities, a governance framework to achieve the objectives and priorities set, the identification of preparedness, response and recovery measures, including collaboration between the public sector and the private sector, the indication of training, awareness and education programs, research and

development plans and a risk assessment plan, the designation of one or more competent authorities to control the application of the directive at national level and of a single point of contact, to ensure international cooperation and connection with other states through the cooperation mechanisms identified in the directive itself.
Finally, each state must designate one or more Computer Security Incident Response Teams (CSIRTs) responsible for monitoring incidents at the national level, providing timely alerts and announcements with the aim of disseminating information on risks and incidents.
Cooperation among institutions of the individual Member States is a crucial part of the NIS directive. To this end, a cooperation group consisting of representatives of the Member States, the Commission and ENISA was set up with four areas of work - planning, guiding, reporting and sharing.
The last of the main points of the directive concerns operators of essential services for the nation and providers of digital services. In particular, public or private companies operating in energy, transport, banking and healthcare, in financial market infrastructures, in the supply and distribution of drinking water and in the digital infrastructures must adopt security measures able to prevent risk, guarantee the security of systems, networks and information and manage accidents.
As well, digital service providers – that is the digital services online market, online search engines and cloud services (cloud computing) - will be required, according to the NIS directive, to implement appropriate security measures and to notify relevant incidents. In addition to the measures already envisaged for operators of essential services, the NIS Directive prescribes other specific security measures for digital service providers, such as the security of systems and installations, the management of business continuity, monitoring and testing, and compliance with international standards. The transposition process had to be completed in each Member State by May 9, 2018.
In September 2017, the Commission launched the Strategic Plan for Cybersecurity. The Plan aims to increase defense, deterrence and the resilience of information systems, based on 3 fundamental pillars: 1) building a resilient European system increasing the level of cybersecurity in the European Union; 2) creating an effective and univocal response to computer crimes, adapting penalties to the seriousness of the criminal action; and 3) encouraging international collaboration.
One of the most important aspects of the proposal concerned the creation of a European Agency on Cybersecurity - the result of the strengthening of the already existing European Information Security Agency and of the Networks (ENISA) – with a full and permanent mandate, with more tools and targets, to come into effect by 2020, when the current Agency mandate will expire. Ongoing training in security systems tops the objectives. The Agency will simulate computer attacks to allow Member States, in coordination with the European institutions and their agencies, to prepare forms of response to potential attacks, improving information and intervention times, thanks also to the creation, in 2018, of a platform for training.

The EU plan also aims to create a single system certification of cybersecurity to overcome the fragmentation currently existing in the presence of 4 main certifications (CPA, CSPN, BSPA, SOG-ISMRA) and to increase reliability, in terms of security, of purchased products.
On this topic, the Commission identified 3 priority areas - security in critical or high-risk applications, cybersecurity in widely-deployed digital products, networks, systems and services used by private and public sector alike to defend against attacks and apply regulatory obligations and the use of "security by design" methods in low-cost, digital, interconnected mass consumer devices which make up the Internet of Things. At the same time, the Commission underlined the specific issues of specific sectors and so, the necessity to encourage the development of their own approach and the definition of sector-specific cybersecurity strategies in areas such as financial services, energy, transport and health.
The Commission also underlined the importance of skills. In fact, effective cybersecurity relies heavily on the skills of the people concerned. Therefore, cybersecurity education at all levels must be developed. Consequently, the Commission encouraged Member States to maximize the availability of cybersecurity tools for businesses and individuals, accelerate the use of more cyber-secure tools in the development of e-government and also draw full benefit from the competence network, and make cyber-awareness a priority in awareness campaigns.
Last, but certainly not least, the carrying out of an effective investigation and prosecution of cyber-enabled crime and a review of the criminal policy in the Member States. Here, the Commission encourages greater uniformity in the penalties applied in the Member States and the affirmation of the right of access to information by the victims of such crimes. It offers an adequate and simple assistance system and the creation of a close collaboration within the Union's judicial system, through strengthening existing structures and local Contact Points.
On 8 March 2019, the Commission and the High Representative proposed the establishment of a horizontal sanctions regime to counter cyberattacks. The proposed regime has worldwide coverage and will enable a flexible EU response irrespective of the location from which cyber-attacks are launched and regardless of whether they are carried out by state or non-state actors.
In the same period (12 March 2019), the "*EU-China – A strategic outlook*" identified some actions to be endorsed by the European Council underlining the importance to safeguard against potential serious security implications for critical digital infrastructure and to detect and raise awareness of security risks posed by foreign investment in critical assets, technologies and infrastructure.
Regulation n. 2019/452 of 19 March 2019 (applicable from 11 October 2020) establishing a framework for the screening of foreign direct investments in the Union, provides a powerful tool to detect and raise awareness of foreign investment in critical assets, technologies and infrastructure. It will further allow for identifying collectively and addressing security and public order threats posed by acquisitions in sensitive sectors.

Considering the importance and the impact of 5G networks and the critical issues on security, on 26 March 2019, the European Commission recommended a set of operational steps and measures to ensure a high level of **cybersecurity of 5G networks** across the EU. The Recommendation sets out a series of operational measures, encouraging Member States to conclude a national risk assessment of 5G network infrastructures by the end of June 2019 (considering various risk factors, such as technical risks and risks linked to the behavior of suppliers or operators, including those from third countries), underlining that EU Member States exclude companies from their markets for national security reasons, if they do not comply with the country's standards and legal framework, supporting exchange of information and the activity of the Commission and the European Agency for Cybersecurity (ENISA), also completing a coordinated risk assessment by 1 October 2019. In the field of cybersecurity, considering that the future European cybersecurity certification framework for digital products, processes and services foreseen in the Cybersecurity Act (which will be discussed later in the analysis) should provide an essential supporting tool to promote consistent levels of security, the Recommendation encourages Member States to immediately and actively engage with all other involved stakeholders in the development of dedicated EU-wide certification schemes related to 5G. In the field of telecoms, it underlines the necessity for Member States to ensure that the integrity and security of public communications networks are maintained, with obligations to ensure that operators take technical and organizational measures to appropriately manage the risks posed to security of networks and services. ENISA will complete a 5G threat landscape that will support Member States in the delivery by 1 October 2019 of the EU-wide risk assessment and by 31 December 2019, the NIS Cooperation Group should agree on mitigating measures to address the cybersecurity risks identified at national and EU levels.

On 7 June 2019, **Regulation n. 2019/881** of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification, and repealing Regulation n. 526/2013 (**Cybersecurity Act**), was published in the Official Journal of the European Union. It entered into force on 27 June 2019 (with the sole exception of a few articles - 58, 60, 61, 63, 64 and 65 - which relate to the national cybersecurity certification authorities, to the conformity assessment bodies and to the establishment of the European Group for the certification of cybersecurity (ECCG), which will enter into force on 28 June 2021).

It gives ENISA a permanent mandate, strengthening its role (art. 1-45), and defines an EU framework for cybersecurity certification, boosting the cybersecurity of digital products and services in Europe (art. 46-65).

The Cybersecurity Act aims to strengthen **the role of ENISA** setting a permanent mandate and allowing it to perform not only technical consultancy tasks, as it has done until now, but also activities to support the operational management of IT incidents by Member States. In this way,

ENISA will be able to guarantee more concrete support, also regarding the implementation of the NIS Directive. The Regulation attributes specific powers and competences to ENISA to develop and implement Union policy and law, encourage operational cooperation at Union level, knowledge and information, public awareness of cybersecurity risks and education, international cooperation, research and innovation and defines the organization of ENISA in also setting specific rules on its budget.

ENISA will also support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, playing a leading role in managing the certification system introduced by the Cybersecurity Act. ENISA will prepare a candidate scheme after consulting with all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process and maintain a dedicated website providing information on, and publicizing, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity. The Regulation fixes security objectives of European cybersecurity certification schemes, namely: a) to protect stored, transmitted or otherwise processed data against accidental or unauthorized storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process; b) to protect stored, transmitted or otherwise processed data against accidental or unauthorized destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process; c) to ensure that only authorized persons, programs or machines are able to access the data, services or functions to which their access rights refer; d) to identify and document known dependencies and vulnerabilities; e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom; f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom; g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities; h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident; i) to ensure that ICT products, ICT services and ICT processes are secure by default and by design; j) to ensure that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

The same regulation also prescribes the publication, by ENISA, on a website of European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity, including information with regard to European cybersecurity certification schemes which are no longer valid, to withdrawn and expired European cybersecurity certificates and EU statements of conformity, and to the repository of links to cybersecurity information. The following art. 54 instead sets out the elements of European cybersecurity certification schemes.

The Regulation also prescribes to Member States the designation - and the following communication to the Commission - of one or more national cybersecurity certification authorities in its territory (whose powers and competences are specifically fixed by art. 58) or, with the agreement of another Member State, the designation of one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State and the allocation of adequate resources to exercise their powers and to carry out their tasks in an effective and efficient manner.
The Regulation identifies the powers and composition of the **European Cybersecurity Certification Group** (art. 62). It is made up of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities (a member of the ECCG cannot represent more than two Member States) and has different tasks to support, propose and cooperate with ENISA and Commission to facilitate the achievement of the objectives set by the regulatory framework.
Finally, the Regulation sets the evaluation by 28 June 2024, and every five years thereafter, by the Commission, of the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need to modify ENISA's mandate and the financial implications of any such modification.

8. POLICY RECOMMENDATIONS

The Next Digital Single Market Strategy

- The EU institutions and national governments should act in order to close the gap across the EU countries, especially in certain areas such as skills and the integration of digital technology into businesses.
- Data regulation should be adapted in order to make more room for experimentation and innovation.
- Once the rules are set, the next priority for the European Digital Single Market should be to encourage public and private investments in the quintessential technologies.
- The establishment of a truly single EU market for seed and venture capital is paramount to a thriving digital ecosystem.
- The E-commerce Directive should be reshaped and upgraded to include new developments, particularly regarding intermediary platforms and industrial IoT.

Connectivity

- New targets, focusing on bringing Internet access with a capacity of at least 100 Mbps to all European households, as well as connecting, with a performance of up to 1 Gigabit, the main socioeconomic drivers (such as schools, hospitals and other PA entities) and covering all urban areas

and major terrestrial transport paths with a 5G signal, should be achieved by using efficiently private and public financial resources.

- Ensuring an investment-friendly ecosystem and guaranteeing the harmonization of rules would be two necessary conditions for attracting massive capital.
- Tools such as the Connecting Europe Broadband Fund and the Connecting Europe Facility (CEF) should be endowed with adequate funding.
- The digital divide between and within Member States should be urgently addressed, also with the contribution of EU cohesion funds.
- Regarding 5G, it is worth noting that spectrum allocation is very far from been complete, with only less than 15% auctioned by September 2019. National governments should be strongly encouraged to complete auctions as soon as possible and allow for a fast roll-out.
- Specific financial measures to support connectivity demand and so investment returns should be envisaged and allowed to proceed smoothly according to EU state aid rules under clearly set conditions.

Data Driven Innovation

- EU governments should consider opening datasets and creating a suitable regulatory environment for adopting and fostering innovation.
- They should also remove barriers to the distribution and use of government data and, at the same time, encourage private entities to disclose data in order to improve market efficiency or solve fundamental market failures.
- In addition, governments should act as both DDI consumers and suppliers. As consumers, they could digitize work processes, digitally interface with citizens and customers and implement a data-driven decision making. As suppliers, they should implement open government policies by being transparent, engaging and accountable, while managing the trade-off between privacy and national security issues and government benefits.
- Where needed, governments could also consider drawing upon direct incentives (in the form of tax credits or other money-equivalent forms) to encourage companies to take the necessary steps to implement DDI.
- The application of data protection rules should be balanced with the necessity to support the evolution of digital services.

A European-Centric AI

- The EU priority is to foster competitiveness and innovation while assuring the drawing up and the enforcement of the legal framework. AI needs to respect the values on which the European Union is based, such as fundamental citizen rights and ethical principles.
- In order to fully reap the AI benefits, the EU should first of all ensure that the right enablers are in place to support the spread of AI (including the rapid rollout of high-load data infrastructures, such

as 5G), progress in the Digital Single Market by reducing fragmentation in terms of telecoms networks, regulations, and the development of an appropriate ethical framework for the inclusive and beneficial use of AI. It should also develop thriving AI-based ICT, by reinforcing early digital development, by making public institutions among the first and largest clients for new technologies and by hindering excessive fragmentation, thus benefitting from the effects of a more global network.

- Investments in AI research and production by both public and private entities should be hugely increased and pooled at the European level. Member State governments should set the right example by committing adequate resources in their national strategies.
- Cooperation with the industrial sector is fundamental, as a way to be more successful in a world that will be increasingly competitive in AI. To do so, the Commission calls for an increase in the level of investments at the national level for the industrial sector, complementing the initiatives undertaken at the European level in the broader framework of Horizon Europe.
- Europe undeniably has many strong assets, including an increasing number of thriving digital hubs and a large group of world-class research institutions. However, it needs to tackle its fragmented AI ecosystem and retain top talents (possibly attracting more from abroad). In this respect, the setting up of a European Institute for AI could play a very significant role.
- Another important aspect for the EU is to foster the right talents and skills not only in research but also in adoption. Digital innovation hubs should play a fundamental role especially for SMEs to access the relevant knowledge needed for the transformation implied by AI.

Impacts on (current and future) Jobs

- The EU should strongly encourage education and training in the field of AI, as well as inter-disciplinarity, by creating dedicated education tracks in formal education institutions and establishing suitable professional qualification programs and, at the same time, by promoting mixed university degrees, where traditional topics are taught side by side with AI-related topics.
- Retraining current workers – especially the less qualified - whose roles would become otherwise obsolete and who need to gain new skills and be redirected towards higher added value activities, needs to be the new mission for training policies.
- For all jobs, current and future workers need to be taught how to collaborate with machines.

Impact on Consumers

- E- commerce has taken on an important role in the economies of the EU countries. To manage this phenomenon, institutions should adopt specific laws for this sector. To safeguard digital consumers, institutions must improve price transparency and strengthen the enforcement of consumer rights and guidance to clarify what qualifies as an unfair trading practice in the digital world.

- The Internet has given consumers access to a range of digital comparison tools (DCTs) and aggregation and intermediary platforms that can filter, parse and curate market information, and can do so in accordance with preferences and parameters set by the consumer. Public institutions need to pro-actively ensure that these services work effectively, contributing to lowering transaction costs and delivering better deals, by enabling consumers to conveniently and efficiently compare and choose between offers from across the market.
- For consumers to have confidence in and benefit from the internal market digital dimension, they must have access to simple, efficient, fast and low-cost ways of resolving disputes which arise from the sale of goods or the supply of services online. This is particularly important when consumers shop cross-border (something they currently do insufficiently). The availability of a reliable and efficient online dispute resolution system could greatly help in achieving this goal.

Cybersecurity

- Today, there is an extremely fragmented cybersecurity approach among the EU Member States. National governments need to understand that only a united and coordinated Europe can better guarantee their citizens and businesses protection from cyberattacks coming from both within and outside the EU.
- This fragmentation partly results from a lack of expertise, staff and integrated national systems. This is particularly troubling because Member States with less advanced capabilities are a "backdoor entrance" into the EU digital market and present security risks for Europe as a whole. The clear vulnerability resulting from this degree of fragmentation makes the proposal for a European competence center paramount.
- The central goal of a European competence center would be to better coordinate European cyber practices by increasing the capacity of all Member States to monitor, prevent, and respond to cybercrime. However, Europe must also address the overall lack of skills that have warranted the need for a center in the first place. Europe's struggle to recruit and maintain young talent has been a problem. Plans to provide incentives for educated youth labor to stay in Europe must be developed to ensure the necessary labor force to protect Europe's cyber landscape. One approach should include investments in startups, to allow for the burgeoning of new technologies and practices, as well as a procurement policy primarily addressed in this area to EU-based companies.