Impact of the INDUSTRY 4.0 on the internet and personal data protection

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Sumary

Figures and tables

DEEP ANALYSIS AND CATEGORIZATION OF THE CONNECTION INDUSTRY 4.0 AND PERSONAL DATA PROTECTION, GDPR, WEB AND DATA SECURITY, WITH THE VIEW FOR THE FUTURE YEARS

1. INTRODUCTION

Industry 4.0 is the evolution to cyber-physical systems, representing the fourth industrial revolution on the road to an end-to-end value chain with Industrial IoT and decentralized intelligence in manufacturing, production, logistics and the industry. It describes a world where individuals move between digital domains and offline reality with the use of connected technology to enable and manage their lives. It is triggering rapid social and economic changes in an unprecedented context of global competitiveness and demographic change.

Three differentiating factors:

- Velocity: The world is more connected and this revolution is transforming everything faster than the other three revolutions.
- Scope: The convergence of digital technologies with advances in several areas means that we are experiencing the emergence of new ways of life. So, technology is changing what it means to be human.
- Systems Impact: Their progresses are so interconnected and sophisticated that they are transforming our society and countries.

The Industry 4.0 has been described as the ‘smart’ factory of the future where computer-driven systems monitor physical processes, create a virtual copy of the physical world and make decentralised decisions based on self-organisation mechanisms, it is focused on the digitalization of processes and in system integration, with application to the traditional industry, with the multiple partners in the value chain.

It is characterized by the digital transformation with the development of cyber-physical technologies that allow disruptive changes in production and business models.

It consists of merging production methods with the latest developments in information and communication technology. This development is driven by the digitalizing trend in the economy and in society. The technological support of this development is made possible by intelligent and interconnected “cyber-physical systems” (CPS) that will enable people, machines, equipment, logistics systems and products to communicate and cooperate directly with one another.

The main factors of the stunning changes we are living include the decreasing cost of computing and connecting devices and the facility to implement AI algorithms. So, in some ways we can predict the opportunities that comes with the fourth industrial revolution:

1. Lower barriers between inventors and markets,
2. More active role for the artificial intelligence (AI),
3. Integration of different technics and domains (fusion),
4. Improved quality of our lives (robotics) and
5. The connected life (Internet)

1.1. TEN TECHNOLOGIES OF THE FOURTH INDUSTRIAL REVOLUTION

- Technologies that change the physical world:
  - Biotechnology.
  - Robotics.
  - 3D Printing.
  - New materials.
  - Internet of Things (IoT).
  - Transmission, storage and energy.
- Technologies that change the digital world:
  - Artificial Intelligence (AI).
  - Blockchain.
  - New computational technologies.
  - Virtual and Augmented Reality.

1.2. GLOBAL IMPACT

- To increase productivity. Technologies such as AI and automation have increased our production capacity and improved the distribution of our time. However, it's not all that simple. There are still many moral and ethical questions about these innovations.
- To reduce barriers between inventors and markets due to new technologies.

- Increasing trends in artificial intelligence point to significant economic disruptions in the coming years. Artificial systems that rationally solve complex problems pose a threat to many kinds of employment, but also offers new avenues to economic growth.
- Innovative technologies will integrate different scientific and technical disciplines. Key forces will come together in "a fusion of technologies that is blurring the lines between physical, digital, and biological spheres. "Fusion is more than complementary technology, because it creates new markets and new growth opportunities for each participant in the innovation. It blends incremental improvements from several (often previously separated) fields to create a product.
- Robotics can and will change our lives in the near future. Technically robots are automated motorized tools. Customized robots will create new jobs, will improve the quality of existing jobs, and give people more time to focus on what they want to do.
- The Internet of things (IoT) is the Internetworking of physical devices. Typically, the IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications.

1.3. MAIN CHARACTERISTICS

Industry is diverse and moving at different speeds. While in general digital transformation strategy has been missing and initiatives have been ad hoc, things are changing in some areas but as we'll see a holistic picture is still missing and the goals remain relatively traditional and isolated.

These set of changes that is experiencing industries are spreading out throughout the whole economy. This is essentially characterised by the introduction of digital technologies in the most diversified fields of economics and society. This is mainly due to increasing automation, digital transformation, the bridging of digital and physical environments evolving industrial and manufacturing technologies, the intensive usage of data/analytics, industry and manufacturing challenges, human, economic and societal evolutions and demands and the integration of information technology and operational technology.

For these reasons above It is necessary to make an effort and provide the companies with the adequate resources to transform their opperativity thus ensuring that companies are able to take advantage of the multiple benefits associated with Industry 4.0 and, simultaneously, neutralizing the challenges and obstacles which are also associated with it.

From a technological viewpoint it's especially in the integration of various technologies that important fourth industrial revolution evolutions occur and are expected. These new technologies are:

- Information and communication technology: (ICT) refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, and network-based control and monitoring functions. Digitalization and the application of ICT allow the integration of all systems throughout the supply and value chains and enables data aggregation on all levels. information is digitized and the corresponding systems inside and across companies are integrated at all stages of both product creation and use lifecycles;
- Cyber-physical systems: Cyber-physical systems are integrations of computation, networking, and physical processes whose main purpose is to control a physical process and, through feedback, adapt itself to new conditions, in real time;
- Network communication: Both within the manufacturing plant and across suppliers and distributors need to enable a communication relationship. So they use technologies, networks and protocols to communicate. This high level of networking of interconnected components allows for a decentralized and self-organized operating of the cyber-physical systems;
- Big data and cloud computing: the information can be used to model, virtualize and simulate products and manufacturing processes; Big data is high-volume, -velocity and -variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making;
- Modelling, virtualization and simulation: Simulation is a core functionality of systems by means of seamless assistance along the entire life cycle, for example, by supporting operation and service with direct linkage to operation data;
- Improved tools for human-computer interaction and cooperation: To control these processes, human workforce is supplied by integrating this technology. The system assists humans in their everyday jobs. The key features of such systems are non-intrusiveness, context-adaptiveness, personalized, location-based and mobility.

2. INDUSTRY 4.0

2.1. MANAGING INDUSTRY

The 4th industrial revolution brings digital tools for an easy and automated analysis of the large amount of operational data circulating in an organization which, because of its large volume, hides relevant knowledge about the operational management of its activity. Therefore, it is important to be aware that there are also some important challenges associated with Industry 4.0. We are going to analize:

- Security. Security risk is probably the main challenging aspect of implementing Industry 4.0 techniques. The integration of these new technologies have to handle with several risk

as security breaches, data leaks and might even involve cyber theft. As data is collected throughout the supply chain questions of ownership will arise and, it is important for companies to make sure that their data won't end up in the ends of a competitor. New operational risk for connected, smart manufacturers and digital supply networks appears, and this is cyber. The interconnected nature of Industry 4.0-driven operations and the pace of digital transformation mean that cyberattacks can have far more extensive effects than ever before. On the other hand, it must be ensured that the production facilities themselves do not pose a threat to humans or the surrounding environment, and that the workers receive continuous safety trainings.

- Privacy. This issue concerns the customers that need to collect relevant data and feel that their privacy is being threatened and also the producers that have to share data using a more transparent environment. Bridging the gap between the consumer and the producer will be a huge challenge for both parties.

2.2. EU & NATIONAL LAW DATA PROTECTION AND IT SECURITY

2.2.1. Introduction

With the rapid digital changes and the increasing needs of the sector, many of these systems are now outdated and incapable of facing new threats brought by the introduction of the internet in factories. The problem is that many companies, still today, are not ready to face such attacks and that their systems and production remain compromised. Within this context, digital industrial platforms play a key role. They help factories throughout the world to connect to their suppliers and customers. However, working in such a hyper-connected environment raises concerns about vulnerabilities, as companies do not want their operational data to be visible to other companies in their supply chain, unless specifically designed for and controlled. Therefore, digital industrial platforms must ensure security by design and by default, putting in place a control framework that includes continuous monitoring. They must support manufacturing companies with increased transparency, interactions with the larger ecosystem, efficiency, and innovation.

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. The Agency is located in Greece with its seat in Athens and a branch office in Heraklion, Crete.

ENISA is actively contributing to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market.

The Agency works closely together with Members States and private sector to deliver advice and solutions. This includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies

on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat landscape, and others. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to NIS.

Securing network and information systems in the European Union is essential to keep the online economy running and to ensure prosperity. The European Union works on a number of fronts to promote cyber resilience across the European Union. The current role of governments is in setting out policies and strategies supporting the digitalisation of the market, regulating the market by setting out legislation (CIP, NIS, GDPR, …) and influencing sector regulations, by issuing operating schemes and providing licences, and by financing research and development and stimulating innovations.

Cyber risks in the age of Industry 4.0 extend beyond the supply network and manufacturing, however, to the product itself. As products are increasingly connected both to each other and, at times, even back to the manufacturer and supply network cyber risk no longer ends once a product has been sold.

The technological developments which are at the base of Industry 4.0 do raise at the same time a vast number of associated of security concerns. Industry 4.0 means opportunities and challenges. Integrating the concept within an organisation means opening up the company’s IT infrastructure, making it more susceptible to errors and more vulnerable to attacks. Therefore, an integrated approach to protecting devices must be taken.

Unfortunately, intruders will not stop trying to find new ways of breaking into business networks. Attacks specifically designed to penetrate industrial control systems present a threat to production facilities. Infected computers can be controlled remotely and their data stolen. Other linked or built-in devices such as microphones, keyboards and monitors can also be spied on. As the malware exploits unknown security holes, firewalls and network monitoring software are unable to detect it. The targets in the smart factory primarily focus on the availability and integrity of the physical process rather than confidentiality of information, as with traditional cyber risks.

The nature of cyber risks in Industry 4.0 thus is largely dependent on the particular industrial portfolio and therefore requires adequate action from the concerned industrial decision making factors. However, given the fact that industrial production is governed by a number of regulations industrial cyber risks should also be a concern for regulators. A wide range of managed expert services is also available. Automation technology and application providers are making additional efforts to provide cybersecure systems, on the basis of self-assessments and joint self-regulation

The production methodology of Industrie 4.0 ideally requires that data protection aspects are already included in the planning phase.IT security also serves the purpose of protecting personal data. Data protection law in this respect demands that the technological and organisational

measures are adopted that are required in the light of data protection law and in this respect imposes various conditions.

It is crucial for a company to use digital transformation in its business processes, examining all the legal challenges it may be facing. Legal challenges include risks arising from the integration of external partners in a company's supply chain, in relation to data protection and security. Data protection and IT security should be the responsibility of a company's management, thus, digital transformation will bring new work profiles. Also it will require companies seeking digital transformation to make substantial efforts to master legal changes in data protection, IT security, labor laws and accountability.

The enforcement of the confidentiality rules in the Regulation will be the responsibility of national data protection authorities and laws differs from country to country. Therefore, the task of adhering to the various laws that are being addressed in markets will be complicated.

2.2.2. EU Regulation

2.2.2.1. Standardisation

Standards are essential components of almost all aspects of the organisation and functioning of modern societies including information security. Through the development and adoption of standards, best practices are shared among organisations, integration and interoperability of systems is promoted, complex environments are simplified, and information systems are shielded against cyber threats. Against this background, ENISA elaborated further on the area of privacy standards considering the developments at legislative, policy, and standardisation level.

EU policy makers and European Standards Organisations should promote the development of European input to privacy and cybersecurity standards. While leadership is needed, to drive standardization efforts in this area, the stakeholders' need to be provided with guidance might be met with private initiatives from beyond the EU. In addition, the aforementioned stakeholders should also establish a mechanism to assess the viability of adopting international standards with European (legal) requirements and filter international efforts to match EU levels.

- EU policy makers and European Cybersecurity Certification Group members should promote the endorsement and adoption of privacy and information security standards, including conformity assessment standards specific to privacy matters.
- EU policy makers and European Standards Organisations should further promote coordination, and
- Collaboration with a range of stakeholders throughout the process of standards developments, and
- Standardisation activity.

- EU bodies and competent authorities in the Member States should promote the adoption of a structured approach on the analysis of sector-specific needs with regard to privacy standardisation, especially in information security context and then proceed with the adoption or development of new standards.
- EU policy makers and relevant EU bodies need to be further involved in the standardisation process, so as to define, endorse or affirm potential standardisation goals in the areas of privacy and information security.

Competent bodies at EU and Member State level should further promote their research and standardisation activities to support the realization of Privacy by Design principle.

2.2.2.2. Cybersecurity

The key objectives of the EU Commission in the field of cybersecurity are:

- Increasing cybersecurity capabilities and cooperation.

  The aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level.

- Making the EU a strong player in cybersecurity

  Europe needs to be more ambitious in nurturing its competitive advantage in the field of cybersecurity to ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology, which is interoperable, competitive, trustworthy and respects fundamental rights including the right to privacy. This should also help take advantage of the booming global cybersecurity market. To achieve this Europe needs to overcome the current cybersecurity market fragmentation and foster European cybersecurity industry.

- Mainstreaming cybersecurity in EU policies.

  The objective is to embed cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids and the loT.

Currently cybersecurity policy framework within the EU is defined by the EU Cybersecurity strategy. The aim was to better protect Europeans online. As the Strategy states, information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems.

Governments can intervene by issuing regulations preventing things that could cause harm to citizens and protecting the public. Regulations can support protection in places where needed. These can take various forms, such as regulating manufacturers, integrators and operators, by issuing operating schemes and providing licences. Governments can also intervene by financing research and development, stimulating further innovations in the domain, or support self-regulation. Government intervention should prevent manufacturers from losing data and money, potentially losing lives, from operational disruption, supporting interactions and innovations, detecting and preventing crime, while at the same time continuing to support the further growth and development of the European Digital Single Market.

2.2.2.3. Data Protection

The General Data Protection Regulation (GDPR) require that it is processed transparently. The 25th of May 2018 is the day that all data protection arrangements in companies have to be changed accordingly, without exceptions. The GDPR does not only affect European businesses, but every company or organization that processes personal data of European citizens. The purpose of processing has to be clear and legitimate. The amount of processed data has to be kept to a minimum, depending on the purpose. The data has to be accurate and the storage time has to be limited to a period that is bound to the purpose. Additionally, integrity and confidentiality of the data have to be protected. In short:

- Lawfulness, transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality.

With the new GDPR it becomes more important to inform the customer, or the person whose data you process, about what happens to their data. What you have to be aware of is summed up in the following points:

- Transparency.
- The right to disclosure of the subject.
- Right to erasure: The ‘right to be forgotten’.
- Right to restriction of processing.
- Right to data portability.
- Right to object.

2.2.3. Portugal

2.2.3.1. Context

The national initiative Indústria 4.0 presented in January 2017, is part of the National Strategy for the Digitalization of the Economy. The overall objective of the National Strategy for the Digitization of the Economy includes an initial set of measures of valorisation, promotion and investment in the digitization of the Portuguese economy. The Ministry of the Economy, intending to generate the conditions for the development of the national industry and services in the new paradigm of Digital Economy, decided to launch an initiative to identify the needs of the Portuguese industrial fabric in the scope of its digital transformation and guide measures (public and private) of awareness, adoption and massification of new technologies in the business models of Portuguese companies. According to the European Commission's Digital Economy & Society Index 2017, Portugal stands above the EU average at the level of digital competitiveness. The Portuguese score has grown at a faster pace than the US average in recent years, currently occupying 16th place

2.2.3.2. Goals

The national initiative has the following core goals:

Table 1. Portugal: goals Indústria 4.0

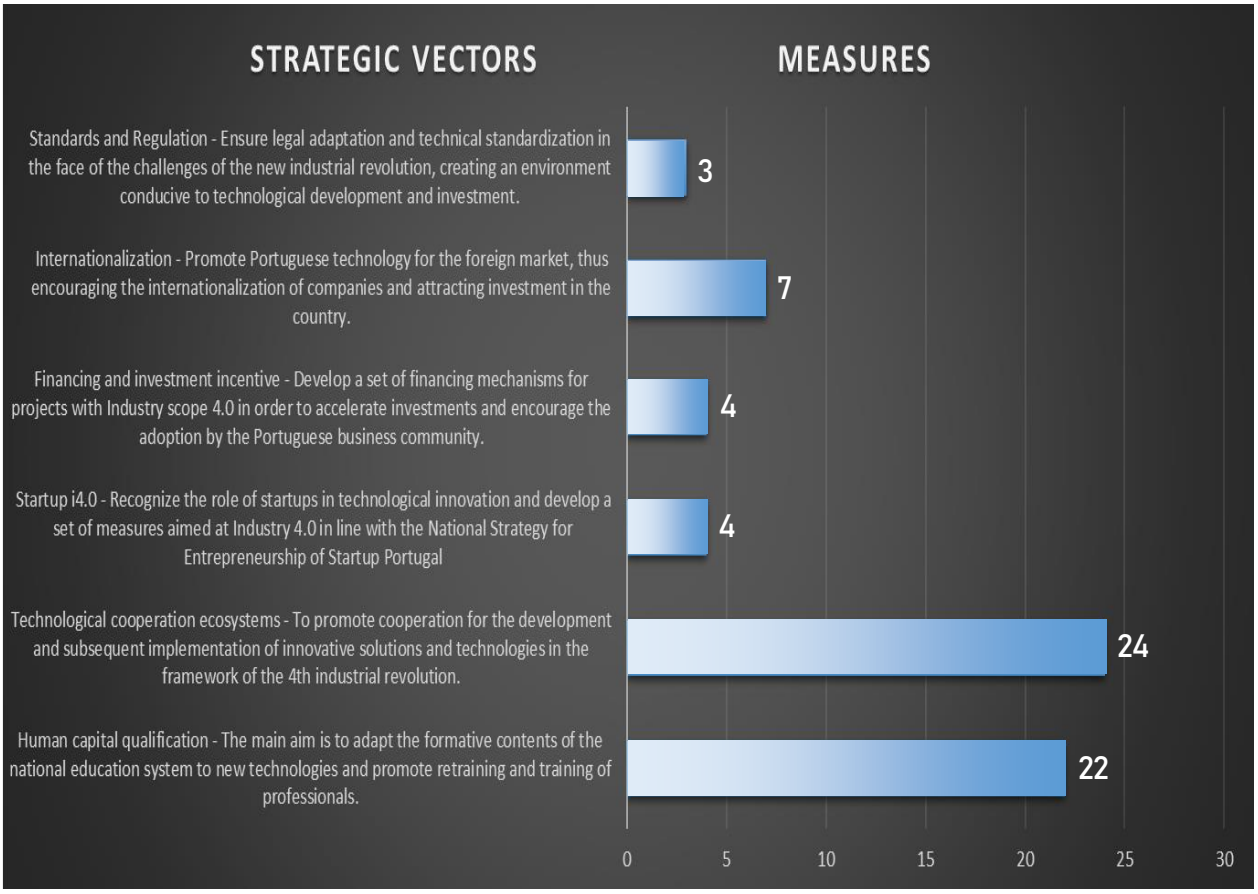
Indústria 4.0	
Accelerate Industry 4.0 concepts and technology adoption	• Provide the business community with knowledge and information • Promote a set of tools for business transformation • Empower and readjust the national workforce
Promote Portuguese companies as international Industry 4.0 players	• Capitalize the scientific and technological ecosystem Analysis of National Initiatives for Digitising Industry • Create a favourable context for the development of i4.0 startups • Promote national technological solutions abroad
Make Portugal an attractive location to invest in Industry 4.0	1. Communicate the country as a HUB of experiences and know-how sharing in order to attract resources 2. Create favorable conditions (legal and fiscal) for investment related to i4.0

The Strategy for Industry 4.0 is a set of 64 public and private initiative measures that are expected to impact more than 50,000 companies operating in Portugal and, at an early stage, will enable the retraining and training of more than 20,000 workers in digital skills.

2.2.3.3. Strategic Lines

The consultation and cooperation process in the field of industry 4.0, identifying key challenges and potential policy and digital enablers led to the definition of 64 measures for the national strategy organised in 6 strategic vectors:

Figure 1. Portugal: strategic lines



In addiction, following the EU guidelines Portugal will be able to implement the General Data Protection Regulation (GDPR) from the 25th May 2018. There are several national guidelines as well as a set number of fines for those who do not follow the rules, including businesses and individuals (General Regulation of data Protection of Portugal, 2018).

It should be noted that the strategy includes the involvement of private sectors as a means to ensure the success of their implementation, and that the initiative depends on an equal

distribution of public and private measures. However, part of the private investment affected is eligible for public co-investment through the Portugal 2020 strategy.

The setting of the Indústria i4.0 Program prioritized the listening/auscultation/sounding of 4 fields of business relevant to the Portuguese economy for their number and importance and their level of preparation for the technological adoption, namely:

- Fashion& Retail.
- Automotive.
- Tourism.
- Agri-food.

Digital Industrial Transformation Enablers. As a result of the digitization of society and industry, the end customer is now more informed and connected with access to a global offer. This phenomenon creates a more competitive environment but with opportunities for better prepared companies. At the disposal of companies are innovative technologies in terms of trade, production and logistics that transform the relationship with the end customer, workers and between companies. The use of available technologies and a customer-focused approach dictate the success of the business fabric in adapting to the challenges of today's markets. The national initiative considers a set of digital transformation enablers (information, connectivity and production) with a vertical impact of the horizontal dimensions of Industry 4.0 (i.e. process, product and business models):

- Information. This digital enabler pillar covers technical domains such as consider aspects such as advanced analytics, artificial intelligence, digital infrastructures, cloud computing & cybersecurity.
- Connectivity. This pillar considers digital enablers such as advanced sensors (including embedded technologies), remote access and system operation and smart machines.
- Production. This pillar considers digital enablers such as advanced materials, modular manufacturing systems, 3D printing and autonomous robotics.

2.2.4. Spain

2.2.4.1. Context

The next technology developments, the increased hyper-connectivity and the globalization of the economy along with the recovery from the financial crisis are bringing important opportunities as well as challenges to the manufacturing domain. Manufacturing industry is increasingly delivering integrated goods and services. They have migrated for the essential delivery of goods towards business models were services play a key role. The Industria Conectada 4.0 (Connected

Industry 4.0 - CI4.0) initiative aims at increasing the industrial added value and quality employment. Developing a unique and competitive model for the industry of the future and promote a strong local offering of digital solutions for the manufacturing sector promoting and enhancing differential competitive levers that favour industry and boost exports. Concerning digitization, Spain ranks 14th in DESI 2017. Spain's performance in the use of digital technologies by enterprises and in the delivery of online public services is above EU average. In Connectivity, progress is particularly strong in terms of subscriptions to fast broadband and NGA coverage is also high. Spanish companies are making progress in integrating digital technologies in their business processes and a fifth of SMEs are actively selling online.

The Spanish strategy is strongly building on the renovation of the manufacturing machinery and development of new digital processes. The strategy is already clearly planning the development of DIH and Platform strategies to make sure that a coordinated action at national level ensures that every Spanish SMEs hold the necessary instruments to establish a digital transformation plan and the access to finance and support from the business innovation stakeholders and competence centres to realise their digital transformation actions. The CI4.0 is supported by additional and complementary set of actions from various Ministries to strengthen the digital skill dimension and to further support the development of new R&I industrial projects.

2.2.4.2. Goals

Connected Industry 4.0 (CI4.0) strategy aims at introducing digital technology in industry to improve the competitiveness of Spanish industry in an increasingly global market with the development of an Industry 4.0 model where innovation is collaborative, the production means are connected, the supply chains are integrated and with digital distribution channels and customer service. All the above in the context of a servitised industry with a smart a customised intelligent product that sets the ground for new business models. The goals of the CI4.0 strategy are:

Table 2. Spain: goals CI4.0

CI4.0
Ensuring widespread knowledge of Industry 4.0 technologies and suitable skill development of Industry 4.0
Encourage digitised collaborative environments and platforms, such as Digital Innovation Hub, Industrial Platforms or Clusters
Enhance the development of digital enablers
Promote industry 4.0 solutions adapted to the industrial needs, including those of SMEs.

Digitization represents a key opportunity to attract international investments and generate quality jobs. CI4.0 strategy aims at leveraging a far-reaching transformation required to ensure that Spain doesn't lag behind in this new industrial revolution.

The Industria Conectada 4.0 will boost digital transformation of Spanish industry by:

- Increasing the industrial added value and quality employment.
- Developing a unique and competitive model for the industry of the future and promote a strong local offering of digital solutions for the manufacturing sector.
- Promoting and enhancing differential competitive levers that favour industry and boost exports.

2.2.4.3. Strategic lines

The strategy responds to four main challenges that Spanish industry will face in their digital transformation:

- Lack of knowledge about the I4.0 initiative.
- Definition of the technologies to use and how to use them.
- Availability of digital enablers.
- The lack of qualified, experienced resources to undertake the transformation, especially in smaller companies

The Digital Agenda introduced measures ranging from improving key production factors with impacts on the competitiveness of industrial enterprises to innovation actions and digital transformation support. As one of the core themes of the Agenda, the digitalisation content included a particular design and implementation that gradually turned into the development of a national strategy.

2.2.4.4. Standardization actions

The Working Group on Standardization of the Connected Industry Initiative 4.0 of the Ministry of Economy, Industry and Competitiveness has been set up in July 2017. This initiative has been created with the aim of promoting the digital transformation of Spanish industry through the joint and coordinated action of the public and private sector. The concept of Industry 4.0 refers to the fourth industrial revolution, characterized by the massive incorporation of information technology to the entire value chain of manufacturing processes. One of the Strategic Areas of the Initiative is devoted to standardization as a fundamental tool for the implementation of the manufacturing model of the future. To meet this need, the Executive Committee of the

Standardization Working Group has been set up, which will be technically coordinated by the Spanish Standardization Association, UNE, and the Mondragon Corporation. It will also include industrial sector associations, companies and universities. The first missions of this working group of standardization will be:

- To make Spanish industry aware of the benefits of participation in the standardization system;
- Increase such participation to the levels of the most advanced countries; and
- The identification of those priority sectors that want to get involved and benefit from this initiative.

Standardization plays a fundamental role in the implementation of Industry 4.0 processes, since a degree of integration between systems of different domains is required, which is only possible if it is based on technical standards and specifications based on consensus. This Working Group is coordinated, from a technical point of view, by UNE (the national organism of standardisation) and Mondragon

2.2.5. Austria

2.2.5.1. Context

The motor of the Austrian economy is the highly innovative and competitive material goods industry. It makes a significant contribution to securing the economic location and the jobs in Austria. Industry 4.0 is regarded as more than just the application of technology to production - it is a conceptual model of new developments based on available and future technologies. Companies need to integrate this model in their strategies to remain competitive. It is expected that intelligent and future-oriented production technologies will strengthen the goods industry in Austria.

2.2.5.2. Goals

The Austrian strategy focuses on targeted investment in information technologies, the development of RTI infrastructures, intellectual property protection and data protection (also in Open Data, Open Science and Open Innovation). About 150 measures of all Ministries, are presented for the first time in a bundled form. The Austrian government also aims at creating framework conditions so that the broad society can benefit from the digitization. New innovative business paradigms, such as Open Innovation are promoted in the course of digitization. Their main objectives are:

Table 3. Austria: goals Industry 4.0

Industry 4.0
To leverage interests between industry, science, policy makers, employers and employees associations
To accompany the processes of change driven by digitalisation
To provide knowledge and services on Industry 4.0 to companies, academia, RTOs and to the general public
To define fields of action and to advise policy makers
To develop joint strategies with high leverage on Industry 4.0
To launch initiatives to steer regional, national and international activities
To enable the exchange of experience, best practices, data and studies

2.2.5.3. Strategic lines

User-driven innovation and crowdsourcing are another focus in the 2017 research and technology report. In January 2017, Austria has also adopted its new government programme for 2017-2018 in which digitisation is identified as one of the key priorities:

1. Austria aims to be a 5G pioneer in the future. A 5G strategy for a new telecommunication infrastructure was announced to be published by the end of 2017.
2. With its Broadband Strategy 20202, the Federal Government is committed to ensuring a well developed and affordable digital infrastructure and provide a comprehensive availability of ultrafast technology (Fiber-to-the-Home FTTH) by 2020. Austria will have to invest around 5 billion Euros. Currently only about 13 % of households use internet connections with at least 30 Mbit/s and only 2% of households have connections with at least 100 Mbit/s.
3. In terms of an innovative and future-oriented school system Austria is committed to a common digitization strategy for schools (“Schule 4.0”).
4. Austria will make digitization a priority during its EU presidency in 2018.

2.2.5.4. Standardization actions

The Working Group of the Platform Industry 4.0 published the Österreichische Normungs-Kompass, Industrie 4.0 (Austrian Standardisation Roadmap Industry 4.0). The aim of the Roadmap is to raise awareness for the topic of standardisation and to give concrete guidance to

relevant stakeholders. The Roadmap is accompanied by an online tool that provides detailed and up to date information on norms and standards that are highly relevant for Industry 4.0 ("Online-Normenkatalog Industrie 4.0"). The Austrian standards Institute (ASI) and The Austrian Association for Electrical engineering (OVE) are the Austrian organizations that drive these activities in the field of standardization. OVE is the official representative at IEC and CENELEC as well as at the National Standards Organisation of ETSI. The organizations work in the following technical fields with relation to Industry 4.0:

- Diagnostics of performance and faults.
- Maintenance.
- Life cycle management.
- System migration.
- Interoperability between systems.
- Development and Engineering (synthesis processes in digital factories).
- Industrial Communication Systems.
- Optimization (e.g. of unstructured data sets).
- Security Management.
- Human-Machine Interaction.
- Modeling Languages (e.g. RAMI 4.0; IoT Reference Architecture).

2.2.6. Czech Republic

2.2.6.1. Context

In light of the highly open Czech economy, it is important for Czech industry to follow and respect the developments in industrially developed foreign economies in the field of digitisation and advanced automation of industrial production and all processes associated therewith. Nevertheless, due to the specific position of Czech industry resulting from the traditionally high level of industrial manufacture in the country's overall economy, the Czech path to the Fourth Industrial Revolution will likely differ from that of foreign economies, as was the case in the previous industrial revolutions. At that time the influence of Czech industry on foreign industry was highly evident and now again we must not miss the chance to be one of the important players.

2.2.6.2. Goals

The goal of the Initiative Industry 4.0 is to show possible trends and outline measures that would not only boost the economy and industrial base in the Czech Republic, but also to help prepare

the entire company society to absorb this technological change. From a policy perspective Průmysl 4.0 provides a profound analysis of I4.0 on society and does not limit itself to a technical evaluation of technologies that will disrupt traditional manufacturing processes and manufacturing systems. It is a holistic and integrated approach that:

Table 4. Czech Republic: goals Průmysl 4.0

Průmysl 4.0
Builds on data and communication infrastructure
Adapts the education system
Introduces new tools in the labour market
To define fields of action and to advise policy makers
Adapts the fiscal support and framework for digital companies

Traditionally the sectors contributing the most to the growth of industrial production are:

- Manufacture of motor vehicles, trailers and semi-trailers,
- Production of rubber and plastic goods,
- Manufacture of electronics, and
- The production of computers, electronic and optical devices and equipment.

2.2.6.3. Strategic lines

The initiative provides an integrated framework dealing with:

- Innovation capacity: Digital Innovation Hubs, Competence Centers, Industrial Platforms, Pilots projects, Test beds. Průmysl 4.0 measures include the support to investment, technological prerequisites and vision, requirements concerning applied research, standardization, safety/security/reliability.
- Actions to promote digital skills: education, vocational training, company involvement, research programmes, academia. It considers the impacts on labour market, skills and social impacts, as well as impacts on education system. It includes measures to support human resources development and life-long learning.
- Complementary measures (e.g. tax incentives, development loans). It deals with cyber security and relevant legislation, application of innovative technologies in energy, transport and Smart Cities. Smart devices & technology innovation.

2.2.6.4. Standardization actions

In the Czech Republic, standardisation is in the purview of the Czech Office for Standards, Metrology and Testing (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví – "ÚNMZ"). Standardisation and the related technical regulations for Industry 4.0 aim at not creating new special standards for each element of Industry 4.0 – that is the job of each sector – but will focus on interoperability of the various elements. The aim is not to create a "Czech standard", but to be included in the European and global process of adopting such standards.

Standardisation is one of the few areas where the Czech Republic can contribute to creating a single, global Industry 4.0 concept. In practice, the majority of standards will be created by big multinational companies, but on the State level, the Czech Republic can become involved in approving and formalising these standards. The Czech Republic has a sufficient number of experts for this; they, however, will have to undergo regular training in this. Průmysl 4.0 initiative proposes that a body be created under ÚNMZ to coordinate the creation and revision of technical standards with regard to the needs of Industry 4.0.

The Průmysl 4.0 standardisation vision puts particular attention into data-driven services and intersectoral topic is ICT services. This topic is influenced by big data and machine processing of certain types of such data, which, for the reason of optimisation in production, will have to be standardised in data structures. The storage thereof in data centres is an important part of Industry 4.0. The threat of destruction, loss, misuse or theft of such data is an extremely important issue. At this time, some standards have been defined for data centres.

The Czech Republic build on a complex regulatory framework that carries on the tradition of its legal predecessors (from the first Czechoslovak Republic, through the war-time Protectorate of Bohemia and Moravia, then the Czechoslovak Socialist Republic to the Czech and Slovak Federative Republic. The composition of its legal code reflects this) it adopted the legislation of its predecessors, with many of them still in force as remnants of a bygone era: since 1918 an estimated 60 000 legal regulations, i.e. acts, decrees and government orders, have been issued within the territory of the Czech Republic. Another 10 000 regulations were taken on from Austria-Hungary in 1918, many of which were never even documented. According to estimates, there are currently around 15 000 regulations in force in the Czech Republic. It is very difficult to do business in such a confused legal environment and implementation. Therefore, as far as the situation in the Czech Republic goes, a possible disadvantage for implementation of Industry 4.0 is the fact that there is no comprehensive national digital strategy and the existing strategic documents are not sufficiently interlinked. Průmysl 4.0 demands a more accessible legal framework that creates no barriers for interoperability and business development and the access to a more integrated framework.

The principles driving smart regulation are as follows:

- Construction preferably digital services (principle “digital by default”). The target is to build all the services so that they can be implemented primarily in electronic form and that, in particular, for the internal functioning of the public administration, the electronic form of mandatorily preferred way to increase efficiency.
- The maximum repeatability and reusability of data and services (principle “only once”). The target is to use information held by public administration so that it may be collected and recorded for their active (re)use. Build services so that they can be re-used for other agendas in public administration.
- Building services accessible and useful to all, including persons with disabilities (the principle of “governance accessibility”). The target is that there will be no discrimination against persons with disabilities. Systems and government services for them will be completely accessible by default.
- Shared government services. The target is to leverage legislation to ensure shared services allowing their use for public administration and other entities.
- Consolidation and interconnection of information systems in public administration. The target is to leverage well, clearly described information systems (incl. their purpose and roles of individual entities). Ensure obligation or option to connect PAIS in order to fulfil the principles of repeatability and reduce the burden on the client, on the contrary, increase the efficiency of public administration.
- International Interoperability - building services connectivity and usable within the European area. The target is to adapt legislation to the requirements of international interoperability and meet the obligations of the data exchange between the EU Member States and promote the use of electronic identification and trust services under Regulation eIDAS.
- Privacy extension to enable quality of service (principle GDPR). The objective is to ensure effective and transparent linking of data resources of public authorities. At the same time ensure full control rights on use of data by data owners concerned.
- Openness and transparency, including open data and services (the principle of open government). The target is to provide legislation to ensure openness to the maximum extent possible, yet ensure the protection of personal data and privacy. Operate an open state services usable without any restriction and publish open data.
- Technological neutrality. The target is not to create artificial barriers limiting the technological neutrality; as opposed to the use of any technical and technological means to restrict the use of specific technologies or even suppliers.
- User friendliness. The target is to leverage legislation to promote the universality and restrict specific user barriers. Also think about the clarity and usability of the digital product as such.

2.3. COUNTRIES COMPARATIVE CHARTS

Table 5. Countries comparative charts

	PORTUGAL	SPAIN	AUSTRIA	CZECH REPUBLIC
CONTEXT	• Indústria 4.0 • Presented in 2017 • Above EU standard (16th place)	• Industria Conectada 4.0 • Above EU standard (14th place)	• Material goods industry • Application of technology to production • Future-oriented production technologies	• Průmysl 4.0 • High level of industrial manufacture
GOALS	• Tecnology adoption • International promotion • Attractive to invest	• To improve competiveness • To create collaborative workflow • SME's adapting to industrial needs	• To accompany the processes of change driven by digitalisation • To define fields of action • To enable the exchange of experience, best practices, data and studies	• Prepare to absorb this technological change and regulate digital and data services. • To make services accessible and useful to all • To share government services
STRATEGIC LINES	• 64 measures in 6 sectors.	• Measures to improve knowledge, technologies, qualified personnel and key production	• 150 measures for a new telecommunication infrastructure, providing a comprehensive availability of ultrafast technology, innovative and future-oriented school system	• To provide an integrated framework dealing with innovation capacity, actions to promote digital skills and complementary measures
STANDARDIZATION ACTIONS	• Information • Connectivity • Production	• Participation • Identefication priority sectors	• Awareness for the topic • To give concrete guidance to relevant stakeholders	• To coordinate the creation and revision of technical standards

				• To pay attention into data-driven services and intersectoral topic is ICT services • To create a more accessible legal framework
EMPOWER	• Fashion& Retail • Automotive • Tourism • Agri-food	• Industrial added value and quality employment • Digital solutions for the manufacturing sector • Boost exports	• Maintenance • Life cycle management • System migration • Interoperability between systems • Security Management • Human-Machine Interaction	• Builds on data and communication infrastructure, • Adapts the education system, • Introduces new tools in the labour market, • Adapts the fiscal support and framework for digital companies.

2.4. EVOLUTION AND FUTURE ON INDUSTRY 4.0

The Industry 4.0 market is poised to grow significantly in the coming years. The increasing adoption of the IoT in the digital transformation of manufacturing and related industries, the rise of industrial robotics and the proportionally higher spend in the Industrial Internet of Things are just some contributing factors.

While we are still in the early days of Industry 4.0 and challenges remain on many fronts such as the integration of IT and OT, data capabilities, implementation challenges, guidelines and strategic capacities, skills, culture, standards and the maturity/readiness levels on the path from sheer optimization/automation to real transformation, Industry 4.0 is also driven by myriad challenges in the supply chain and customer expectations.

The manufacturing industry continues to evolve. Digital transformation is a discussion that has touched every part of the value chain. No matter if you work in design, the supply chain, operations, or service, the adoption of digital capabilities to create business value has become critical to success.

Data is core to digital transformation, and data governance will be required to improve the level of enterprise data integrity in support of digital transformation initiatives. Data governance is a discipline of innovative process, policy, people, data, and technology integrated and incorporated

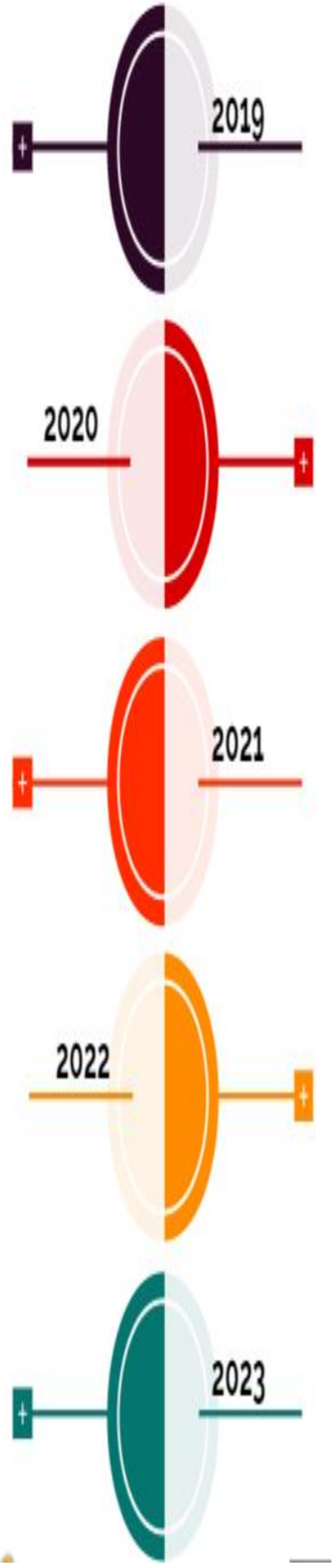
into everyday business operations and strategic decision making, resulting in higher levels of data integrity and better business outcomes.

Regulations such as GDPR will start to be enforced; and organizations are finally realizing the value of data as an asset that needs to be protected, managed and maintained to increase asset value. Because data is a digital asset, and has mostly been managed within the realm of IT, organizations are quick to look at technology, expecting to find data governance software and solutions; but technology is only part of the solution.

A major threat to successful transformation for most businesses remains the failure of their IT organizations to convert from being the back-office enabler of internal business processes to playing a leading role as the engine powering digital business flows between people, things, and data.

Figure 2. Evolution and future on Industry 4.0 2019-2023

80% of enterprises' new digital services will be composite workloads that need secure, reliable interconnection with third-party data/analytic resources in cloud or colocation facilities.
25% of enterprises will shift away from large datacenter consolidation to modernizing optimally located smaller datacenters to support new compute and data-intensive applications.



The need to secure growing volumes of dispersed data generated at edge locations will have driven 40% of enterprises to set up and operate data vaults in multiple colocation facilities.
Most enterprises will shift internal investments to deploy dedicated cloud platforms from which to launch innovative services rather than investing in modernizing existing datacenters.

60% of enterprises will require access to power/cooling infrastructure operating at three times today's standard to manage power-hungry accelerated compute systems' fluctuations and demands..
70% of enterprises will adopt dynamic software-defined branch and network solutions that deliver security and flexibility across cloud, datacenter, and edge interactions.

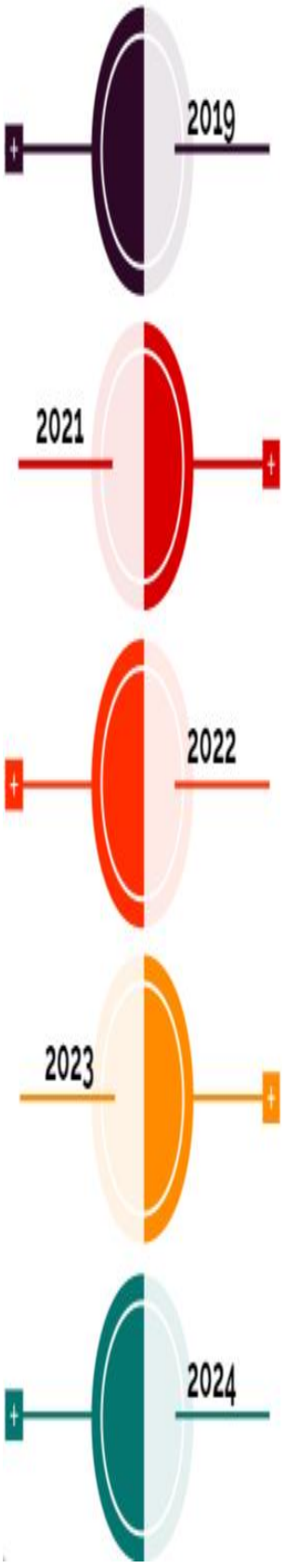
50% of IT assets in enterprise datacenters will have the ability to run autonomously using embedded AI functionality that leverages smart IT and facilities systems.and edge interactions.
40% of enterprises will have doubled their IT asset spending in edge locations and nearby colocation facilities versus core datacenters to deliver digital services to local users and things.
40% of enterprises' spending with colocation providers will be on advanced asset management and optimization services rather than on basic connectivity and facility

60% of enterprises will use flexible, lower-cost IT consumption models that leverage centralized IT asset depots jointly run by hardware suppliers and colocation providers.and edge interactions.

In a digital economy where owning the customer experience is the goal, a premium must be placed guaranteeing response time and rapid but secure data movement. Greater use of data vaults, increasing service interconnect of composite workloads, and the creation of a service delivery edge will dominate datacenter decisions.

Also, we have to consider that the complexity of networks is changing, the adversary becomes better equipped, protection of identity is requisite, and compliance becomes enforceable. For all these reasons, we also see this as a time of opportunity as businesses have various options in products and services that enable them to shape a precise cybersecurity posture that is fiscally attractive and addresses the needs of both security and operations.

Figure 3. Evolution and future on Industry 4.0 2019-2024



DECISION ON SELECTING THE CRUCIAL THEMES AND THEIR SUB-TOPIC FOR THE REPORT ACCORDING TO THE NEEDS-SURVEY AND CRITERIA CATALOGUE DEFINED IN THE FIRST MEETING

Standards are often developed in support of Union policy and legislation. In the field of privacy and information security, reference to standards or acknowledgement of their significance has also been introduced in the EU legislative instruments.

The European Network and Information Security Agency (ENISA) has highlighted several key areas in need of improvement. Cyber threats are a growing menace, spreading to all industry sectors by proving that cyberattacks have a significant impact on critical infrastructures. The road to enhanced data security begins with awareness, according to ENISA officials. While the sector was commended for its regulation of physical security, digital threats can no longer be ignored. As such, member states were encouraged to launch educational campaigns and bolster cybersecurity training frameworks within all shipping companies and port authorities to establish a more holistic defense strategy. The realization of these noble goals will, however, require contributions and cooperation from a variety of sources. Due to the scope and complexity of maritime operations, technology contractors are being called upon to ensure airtight security in their system architecture.

Although global data security awareness is on the rise around the world, the EU has taken perhaps the most proactive stance of any regulatory body. From protecting consumer information against surreptitious online marketing efforts to aligning corporate data protection standards.

Building on the ambitious cybersecurity initiatives announced in 2017, the European Commission proposes as a next step the creation of a Network of Cybersecurity Competence Centres and a new European Cybersecurity Industrial, Technology and Research Competence Centre to invest in stronger and pioneering cybersecurity capacity in the EU.

The mission of the proposal to establish a European Cybersecurity Network and a Competence Centre is to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market. This goes hand-in-hand with the key objective to increase the competitiveness of the EU's cybersecurity industry and turn cybersecurity into a competitive advantage of other European industries.

2.5. CYBERSECURITY ISSUES

By managing the cybersecurity funds under the next multi-annual financial framework 2021-2027, the initiative will help to create an inter-connected, Europe-wide cybersecurity industrial

and research ecosystem. It should encourage better cooperation between relevant stakeholders (including between cybersecurity civilian and defence sectors) to make the best use of existing cybersecurity resources and expertise spread across Europe. The initiative builds on the expertise that already exists in more than 660 cybersecurity expertise centres from all Member States who have responded to a recent survey conducted by the European Commission.

It should help the EU and Member States take a proactive, longer-term and strategic perspective to cybersecurity industrial policy going beyond research and development only. This approach should help not only to come up with breakthrough solutions to the cybersecurity challenges which the private and public sectors are facing but also support the effective deployment of these solutions. It will allow relevant research and industrial communities as well as public authorities to gain access to key capacities such as testing and experimentation facilities, which are often beyond the reach of individual Member States due to insufficient financial and human resources. Furthermore, the proposal will contribute to closing the skills gap and to avoiding a brain drain by ensuring access of the best talents to large-scale European cybersecurity research and innovation projects and therefore providing interesting professional challenges.

The key objectives of the EU Commission in the field of cybersecurity are:

1. Increasing cybersecurity capabilities and cooperation

The aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level.

2. Making the EU a strong player in cybersecurity

Europe needs to be more ambitious in nurturing its competitive advantage in the field of cybersecurity to ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology, which is interoperable, competitive, trustworthy and respects fundamental rights including the right to privacy. This should also help take advantage of the booming global cybersecurity market. To achieve this Europe needs to overcome the current cybersecurity market fragmentation and foster European cybersecurity industry.

3. Mainstreaming cybersecurity in EU policies

The objective is to embed cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids and the loT.

The proposal creates a Network of National Coordination Centres, a Cybersecurity Competence Community and a European Cybersecurity Industrial, Technology and Research Competence Centre. Each Member State will nominate one National Coordination Centre. They will function as contact point at the national level for the Competence Community and the Competence

Centre. They are the "gatekeeper" for the Community in their country support to carry out actions under this Regulation, and they can pass on financial support to national/local ecosystems.

This Community will involve a large, open, and diverse group of actors involved in cybersecurity technology, including in particular research entities, supply/demand-side industries and the public sector. It will provide input to the activities and work plan of the Competence Centre and it will also benefit from the community-building activities of the Competence Centre and the Network.

The Competence Centre will facilitate and help coordinate the work of the Network and nurture the Cybersecurity Competence Community, driving the cybersecurity technological agenda and facilitating common access to the expertise of national centres. The Competence Centre will in particular do so by implementing relevant parts of the Digital Europe and Horizon Europe programmes by allocating grants and carrying out procurements.

2.5.1. Tasks and objectives

The Competence Centre will seek to achieve its overall mission by:

- Setting up and helping to coordinate the National Coordination Centres Network and the Cybersecurity Competence Community;
- Implementing cybersecurity-related financial support from Horizon Europe and the Digital Europe Programme.

That will feed into the following objectives:

- Contribute to the wide deployment of the latest cybersecurity technology, in particular through carrying out or supporting procurement of products and solutions;
- Provide financial support and technical assistance to cybersecurity start-ups and SMEs to connect them to potential markets and to attract investment;
- Support research and innovation based on a comprehensive industrial and research agenda, including large-scale research and demonstration projects in next-generation cybersecurity capabilities;
- Drive high cybersecurity standards not only in technology and cybersecurity systems but also in skills development; and
- Facilitate the cooperation between the civil and defence spheres with regard to dual use technologies and applications, and enhancing civil-defence synergies in relation to the European Defence Fund.

2.5.2. The Directive on security of network and information systems (NIS Directive)

The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member States have to transpose the Directive into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018.

The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
- Cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks,
- A culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

2.5.3. A "NIS Toolkit"

As the cybersecurity threat landscape is evolving fast, it is necessary to swiftly implement the Directive. In view of the impending deadlines for its transposition into national legislation (by 9 May 2018), and for the identification of operators of essential services (by 9 November 2018), the Commission adopted on 13 September 2017 a Communication that aims at supporting Member States in their efforts to implement the Directive swiftly and coherently across the EU.

The "NIS toolkit" provides practical information to Member States, e.g. by presenting best practices from the Member States and by providing explanation and interpretation of specific provisions of the Directive to clarify how it should work in practice.

2.6. PRIVACY ISSUES

The Digital Single Market Strategy ("DSM Strategy") has as an objective to increase trust in and the security of digital services. The reform of the data protection framework, and in particular the adoption of Regulation (EU) 2016/679, the General Data Protection Regulation ("GDPR"), was a key action to this end. The DSM Strategy also announced the review of Directive 2002/58/EC ("ePrivacy Directive") in order to provide a high level of privacy protection for users of electronic communications services and a level playing field for all market players. This proposal reviews the ePrivacy Directive, foreseeing in the DSM Strategy objectives and ensuring consistency with the GDPR.

This proposal is lex specialis to the GDPR and will particularise and complement it as regards electronic communications data that qualify as personal data. All matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR. The ePrivacy Directive is part of the regulatory framework for electronic communications.

To ensure the effective legal protection of respect for privacy and communications, an extension of scope to cover OTT providers is necessary. While several popular OTT providers already comply, or partially comply with the principle of confidentiality of communications, the protection of fundamental rights cannot be left to self-regulation by industry. Also, the importance of the effective protection of privacy of terminal equipment is increasing as it has become indispensable in personal and professional life for the storage of sensitive information. The implementation of the ePrivacy Directive has not been effective to empower end-users. Therefore, the implementation of the principle by centralising consent in software and prompting users with information about the privacy settings thereof, is necessary to achieve the aim. Regarding the enforcement of this Regulation, it relies on the supervisory authorities and the consistency mechanism of the GDPR.

While the GDPR ensures the protection of personal data, the ePrivacy Directive ensures the confidentiality of communications, which may also contain non-personal data and data related to a legal person. The ePrivacy rules still have EU added-value for better achieving the objective of ensuring online privacy in the light of an increasingly transnational electronic communications market. It also demonstrated that overall the rules are coherent with other relevant legislation, although a few redundancies have been identified vis-à-vis the new GDPR.

2.6.1. The principles of the GDPR

The general principles of processing personal data require that it is processed transparently. The purpose of processing has to be clear and legitimate. The amount of processed data has to be kept to a minimum, depending on the purpose. The data has to be accurate and the storage time has to

be limited to a period that is bound to the purpose. Additionally, integrity and confidentiality of the data have to be protected. In short:

- Lawfulness, transparency,
- Purpose limitation,
- Data minimisation,
- Accuracy,
- Storage limitation,
- Integrity and confidentiality.

2.6.2. Rights of the data subject – how companies have to handle personal data

With the new GDPR, it becomes more important to inform the customer or the person whose data you process, about what happens to their data. What you have to be aware of is summed up in the following points:

- Transparency: The data subject has to be able to find out what data is being stored.
- Whoever processes data is obligated to provide the data subject with information. The subject has a right to disclosure.
- Right to erasure: The 'right to be forgotten' is an important addition to the new GDPR. Under clearly defined circumstances the "data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" for example, when the subject withdraws its consent.

> There is a right to restriction of processing.
> In which cases this applies is defined clearly in the GDPR

- Right to data portability: This is new as well. The data subjects have the right to obtain their data "in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller". When "technically feasible" the subject has the right to have the data transmitted from one controller to another. This limitation to technical feasibility is a courtesy to companies, when the transmission of the data would pose disproportionate challenges. However, if the technical requirements are given, this service has to be provided.
- Right to object: For reasons that are defined in the GDPR, a data subject can object to the processing of personal data.

2.6.3. Who is responsible for protecting personal data?

The responsibility to comply with the GDPR lies with companies that process personal data. There have to be "appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation." Examples of these measures are pseudonymisation or encryption. "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary". If the responsible controller is not in the EU, for example when a US company processes data of European citizens, he have to designate in writing a representative in the Union.

2.6.4. Who needs a data protection officer and internal documenta-tion?

Companies have to designate a data protection officer, when one of the following applies:

- When the processing is carried out by a public body (except courts)
- When the core activities of the processer "consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale"
- When special categories of data or "data relating to criminal convictions and offences" are being processed

Companies that process data are obliged to keep records of processing activities, unless they have less than 250 employees. Smaller businesses are not to have any disadvantages because of the new GDPR, therefore "the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation".

2.6.5. ePD description and objectives

- Its first objective is to ensure an equivalent level of protection across the EU of the fundamental right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector. This protection is also granted to subscribers who are legal entities.
- Its second objective is to ensure an equivalent level of protection with respect to the processing of personal data in the electronic communications sector to protect the fundamental right to data protection.

- Its third objective relates to the internal market and is to ensure free movement of personal data processed in the electronic communications sector and the free movement of electronic communications terminal equipment and services in the EU.

These objectives are closely intertwined and rely on one another and supported by a series of specific provisions These specific provisions, each of which pursues one or several of the ePD main objectives, can be classified around 5 main areas harmonised by the ePD, namely:

- Security of electronic communications;
- Confidentiality of communications and related traffic data;
- Confidentiality of information stored in terminal equipment;
- Protection of users (i.e. natural and legal persons) against unsolicited communications;
- Other provisions ensuring users' data protection and the protection of subscribers' legitimate interests

2.6.6. Scope of the ePD

The ePrivacy Directive regulates "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community". In particular, its provisions apply to providers of "electronic communications networks and services". To be covered by the Directive: the service should be an electronic communications service, the service should be offered in an electronic communications network, the aforementioned service and network should be publicly available, and the network or service should be provided in the Community.

2.6.7. Applicable law and cross-border situations

Contrary to the Data Protection Directive, the ePrivacy Directive does not contain an explicit provision with regard to the applicable national law. This may create legal uncertainty as to which law should apply in a cross-border context. In particular, it is unclear whether the rules on applicable law of the DPD apply (country of origin) or whether the ePrivacy Directive should be considered as following the applicable law rules set forth in the directives belonging to the ECS package (country of destination). The unclear situation derives from the lacking of a specific applicable law rule, which hinders an effective application of the rules in a cross-border situation.

2.6.8. Security of electronic communications

The ePD requires providers of electronic communications services to take appropriate technical and organisational measures to safeguard the security of their services (Article 4). In case of a

particular risk of a breach of the security of the networks, the service providers must also inform their subscribers of this risk (Article 4.2). Publicly available electronic communications service providers must also notify personal data breaches to relevant authorities, and in certain cases (if the breach is likely to adversely affect that person) also to the subscribers and individuals concerned (Article 4.3).

Summarizing, the General Data Protection Regulation (GDPR) is an essential tool to safeguard individuals' fundamental right to the protection of personal data in the digital age. It offers businesses simplified rules, creates new business opportunities and encourages innovation. The Commission is working closely with Member States, the independent Data Protection Supervisory Authorities, and with businesses and civil society to prepare for the application of the Regulation from 25 May 2018.

The proposal for a revised ePrivacy Regulation would complement the GDPR while also ensuring alignment with the relevant rules of the GDPR. It will further increase legal certainty and the protection of users' privacy online, while also increasing business use of communications data, based on users' consent. Swift adoption of the ePrivacy Regulation will allow consumers and businesses to benefit from the full digital privacy framework when the GDPR applies in May 2018.

3. THE DIGITAL SINGLE MARKET STRATEGY

The Digital Single Market denotes the strategy of the European Commission to ensure access to online activities for individuals and businesses under conditions of fair competition, consumer and data protection, removing geo-blocking and copyright issues.

A Digital Single Market (DSM) is one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and engage in 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. Achieving a Digital Single Market will ensure that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally.

This Digital Single Market Strategy has benefitted from input and dialogue with Member States, the European Parliament and stakeholders. It has a multi-annual scope and is focused on key interdependent actions that can only be taken at EU level. They have been chosen to have maximum impact, can be delivered during this Commission's mandate, and will be taken forward in line with Better Regulation principles. Each action will be subject to appropriate consultation and impact assessment.

The DSM strategy was adopted on the 6 May 2015. It includes 16 specific initiatives which have been delivered by the Commission by January 2017. Legislative proposals are currently being discussed by the co-legislator, the European Parliament and the Council.

A DSM creates opportunities for new startups and allows existing companies to reach a market of over 500 million people. Completing a DSM can contribute EUR 415 billion per year to Europe's economy, create jobs and transform our public services.

Furthermore, it offers opportunities for citizens, provided they are equipped with the right digital skills. Enhanced use of digital technologies improve citizens' access to information and culture and improve their job opportunities. It can promote modern open government.

Table 6. The DSM Strategy

Pillars	Initiatives
Access: better access for consumers and businesses to digital goods and services across Europe;	• Rules to make cross-border e-commerce easier including consumer protection rights • Better enforcement of consumer rights • More efficient cross-border parcel delivery • To end discriminatory practices in geo-blocking • The renewed approach to apply anti-trust law in the e-commerce sector ▪ • A reform of European copyrights legislation • To increase the access of broadcasting services across Europe • A reduction of the administrative burden of complex VAT procedures in cross-border sales
Environment: creating the right conditions and a level playing field for digital networks and innovative services to flourish;	• An ambitious modernisation of EU telecoms legislation • A review of the audio-visual media framework • An inquiry of online-platforms as dominant player in digital markets from the perspective of competition law • A modernisation of the EU data privacy legislation (e-privacy Directive) • Measures on cyber and network security
Economy & Society: maximising the growth potential of the digital economy.	• The promotion of the free flow of data by a European 'Free Flow of Data Initiative' and a 'European Cloud Initiative' • The definition of interoperability standards in various areas of the Digital Single Market, e.g. e-health, transport planning or energy • An inclusive digital society

In order to ensure a fair, open and secure digital environment, the Commission has identified three main emerging challenges:

- To ensure that online platforms can continue to bring benefit to our economy and society,
- To develop the European Data Economy to its full potential, and
- To protect Europe's assets by tackling cybersecurity challenges.

The digital transformation is structurally changing the labour market and the nature of work. There are concerns that these changes may affect employment conditions, levels and income distribution. Alongside investment in technology, we need investment in skills and knowledge, to be ready for the future. The need for new multidisciplinary digital skills is exploding.

Together with all stakeholders, such as Member States, industry, social partners and education and training providers, the Commission will:

- Address these challenges as part of a comprehensive dialogue on the social aspects of digitisation that engages all stakeholders involved in all aspects of work, education and training.
- Reinforce the role of industry and research organisations in the Grand Coalition and stimulate further commitment from industry to take action.
- Improve the understanding of skills requirements for new technologies, including within H2020, and promote the development of digital skills and stimulate partnerships for skills within the framework of the New Skills Agenda for Europe.
- Engage Digital Innovation Hubs () in skills for mid-caps and.

3.1. INVESTING IN THE DIGITAL SINGLE MARKET

A key aim of the Digital Single Market Strategy is to establish a supportive investment climate for digital networks, research and innovative business. Setting the right framework conditions will help to mobilise private investment and generate investor confidence. Achieving our digital ambitions will require significant investment. EU funding is already earmarked for Digital Single Market infrastructures and services as well as for research and innovative SMEs (including start-ups). Particular efforts are needed to close the digital gap between urban and rural areas. Complementing current EU programmes, the European Fund for Strategic Investments designed to support a wide range of digital projects, in particular due to their high innovation and research component (and thus higher risk). Significant additional funding possibilities are provided by the European Investment Bank and the European Investment Fund.

Innovative entrepreneurs are central to the digital economy. To succeed they need increased access to finance including equity and venture capital. The EU has put in place a range of initiatives to support equity based finance, including regulatory vehicles such as the European Venture Capital Funds Regulation. However, further work is needed to make appropriate financing available as the current diversity of company statutes and related legal risks and costs across Europe tend to inhibit investment in EU start-up ventures and to further scaling up of their business.

Taking into account the experience of past under-absorption of EU funds programmed for investment in ICT, the Commission will work with the European Investment Bank, project promoters and Member States to ensure that available investment funds are fully used, including technical assistance and the full use of synergies between funding instruments.

3.2. INTERNATIONAL DIMENSION

The scale provided by a completed Digital Single Market will help companies to grow beyond the EU internal market and make the EU an even more attractive location for global companies. The openness of the European market should be maintained and developed further in the digital sphere. The EU should continue to press for the same openness and effective enforcement of intellectual property rights from our trading partners. Barriers to global digital trade particularly affect European companies since the EU is the world's first exporter of digital services. To that end an ambitious digital trade and investment policy should be further developed including by means of the EU's free trade agreements. A completed Digital Single Market can also contribute to delivering the post-2015 development agenda. The Commission will work to develop a sustainable approach to Internet Governance through the multi-stakeholder model with the aim of keeping the Internet free and open.

3.3. EFFECTIVE DIGITAL SINGLE MARKET GOVERNANCE

Reflecting the shared responsibility for timely delivery of the actions in the strategy, the Commission will engage with the European Parliament and the Council and deepen its cooperation with both institutions. The Commission will engage in an ongoing dialogue with stakeholders to inform on policy-making and to ensure effective implementation of the Strategy. Given the cross-cutting nature of the Digital Single Market Strategy, its implementation will require the support of dedicated advisory and support groups. The Commission encourages the European Council to provide the necessary impetus and review progress regularly. The Commission will also seek to improve the quality of the data and analysis needed to underpin the Digital Single Market by pooling the relevant knowledge and making it easily accessible to the public. It will further develop its Digital Economy and Society Index indicator. The Commission will report regularly on progress for the Strategy.

4. CONCLUSION

The Digital Single Market Strategy outlined the path for the EU to build the right digital environment: one in which a high level of privacy, protection of personal data and consumer rights are ensured, businesses can innovate and compete, and cybersecurity strengthens the fabric that weaves our societies together.

The strategy for a Digital Single Market is about transforming European society and ensuring that it can face the future with confidence. The Commission invites the European Parliament and the Council to endorse this Strategy to complete the Digital Single Market as soon as possible and to actively engage in its implementation, in close cooperation with all relevant stakeholders.

The openness of the European market should be maintained and developed further in the digital sphere. The EU should continue to press for the same openness and effective enforcement of intellectual property rights from our trading partners.

The key issue is that a society with a high level of data innovation may still be very unequal, with a few actors concentrating most of the power and capturing the benefits. This underlines the role of policies in pursuing a balanced and participative data-driven society, where individuals maintain control of their own data (a key principle of the General Data Protection Regulation, GDPR). In this context, the diffusion of open data is a promising development. While digitization is everywhere, adoption is uneven across companies, sectors, and economies.

This scenario predicts that the current positive economic climate and growth dynamics of the European Data Market will continue towards 2025, driven by a healthy growth of the European data industry, a continuing improvement of the offering of data products and services, and a corresponding gradual development of demand, especially by the most advanced, competitive and innovative enterprises, large and small. Also, it is estimated that over half of EU enterprises are still struggling with the implementation of GDPR (due in May 2018) aiming for pragmatic compliance, while very few are looking at it as an opportunity. We foresee the GDPR to create gradually a successful harmonisation of regulation across the EU, but we suspect that organisations will need a long period of adaptation. Removing barriers to the flow of non-personal data across Europe is a critical success factor to unlock the exploitation of European datasets at a scale and scope sufficient for the new data-driven processes such as machine learning.

Building a Digital Single Market is a key part of the EU's strategy to prepare itself for the future and to continue to deliver high living standards for its population, however the European Commission's initiatives aim to improve online security, trust and inclusion. Trust and security are at the core of the Digital Single Market Strategy. It requires political will and means delivering on the actions set out in this Strategy. It requires mobilising the necessary funds and resources and establishing a governance structure among the key actors to ensure effective

delivery by the EU institutions, Member States and stakeholders. To do so, the Commission intends to unlock the re-use potential of different types of data and facilitate its free flow across borders to achieve a European digital single market. To unlock this potential in the data economy, the EU must take its opportunities to stimulate innovation and in full compliance with data protection legislation.

Three key areas have been identified:

- citizens' secure access;
- better data to promote research;
- digital tools for citizen empowerment.

Where there is already sufficient evidence of barriers that need to be removed the Commission will table legislative proposals and take initiatives to put the scale of the single market at the service of the consumer and business. Where further consultation and evidence gathering is needed in order to identify the right course of action the Commission will engage stakeholders in discussing the options available. This agenda calls for the Commission, Parliament and Member States to work together and to take ambitious steps.