Department of Business and Management

Master of Science in Management Entrepreneurship and Innovation

Chair of Markets, Regulation and Law

Beyond the GDPR: Data Protection in the Context of Industry 4.0

SUPERVISOR

Prof. Granieri Massimiliano

CANDIDATE

Cecilia Proietti-Franceschilli

Matr. 699491

CO- SUPERVISOR

Prof. Colangelo Giuseppe

ACADEMIC YEAR 2018-2019

Table of contents

Introduction

The last years have been dominated by a dramatic growth in the quantity of data that are produced and analysed in a unit of time. The assignment of this thesis is to understand how this phenomenon can become a threat for businesses and individuals and what instruments can be employed to contain the risks arising from these events. These issues are observed from the specific point of view of Industry 4.0, which constitutes an environment that finds in data an important instrument.

The first chapter will provide the reader with an overview on Industry 4.0, that includes the definition of this concept and of its fundaments. From this first analysis, the importance of one element will emerge, i.e. the Smart Factory. It represents the physical and abstract place where all the other phenomena related to Industry 4.0 occur. In the Smart Factory, machines and humans become interconnected through the Internet of Things, causing the production and the processing of millions of bytes of data. While the advantages brought by this combination of technologies are undeniable for what regards the optimisation of the production processing, the challenges of the Smart Factory can be very complex. One of these is data protection.

In the second chapter, the topic of data will be explored. The interest stimulated by this topic, as anticipated before, is strictly related to their growth in Volume, Velocity and Variety. This phenomenon is commonly described by the buzzword Big Data. What changed in the data protection environment because of the advent of Big Data is that the line between two important categories of data, non-personal and personal, has become very blurred. Personal data is data that can lead to the identification of individuals, posing great risks for their privacy. The interest in the Industry 4.0 context derives from the very essence of this environment, characterised by an unprecedented level of the interconnectedness between sensors, machines and humans.

Regardless of the speed of these changes, Europe always managed to keep pace with the threats arising from the use of personal data in different contexts. This is demonstrated by the evolution of the legislative framework, which will be outlined in the last section of chapter two.

The last chapter analyses the possibility of enhancing, with a focus on Industry 4.0, the European data protection framework, that was already improved recently with the enforcement of the General Data Protection Regulation. The starting point is a document published by the Directorate of the European Parliament, that suggested the creation of

an Industry 4.0 Bill of Rights. The need for such an instrument can be explained, according to the author, by the intrusiveness of the technologies employed in the Smart Factory and by the consequent loss of control over personal data.

Thus, the chapter will try to assess the proposal of the Directorate by answering two main questions: what characteristics should this Bill of Rights have? And mostly, is it really needed?

1. Industry 4.0: The Fourth Industrial Revolution

1.1 An Innovative Concept

Through history, human society has witnessed three main technological transitions that became known, due to their abruptness and disrupting effects, as industrial revolutions. The first paradigm shift happened in the late 18th century in Great Britain, when the industry as it is known today was born. From hand production, machine tools were invented and introduced in the factory, also propelled by the extensive use of the steam engine. The second industrial revolution began at the end of the 19th century and was characterised by the introduction of many new technologies. This was facilitated by the expanded usage of more cost-efficient materials, such as steel, by the introduction of electrical power, both in the factory and in the house and by the spread of mass production and labour division, according to the principles of Ford and Taylor. Finally, the third industrial revolution can be traced back to the 70s of the last century and it is also known as Digital Revolution, as it is mainly associated with the invention and spread of digital computers and their associated technologies and with the introduction of the first automated processes in the factory. When reading about these relevant transitions, it is possible to notice that they were all identified and described some years after they took place.

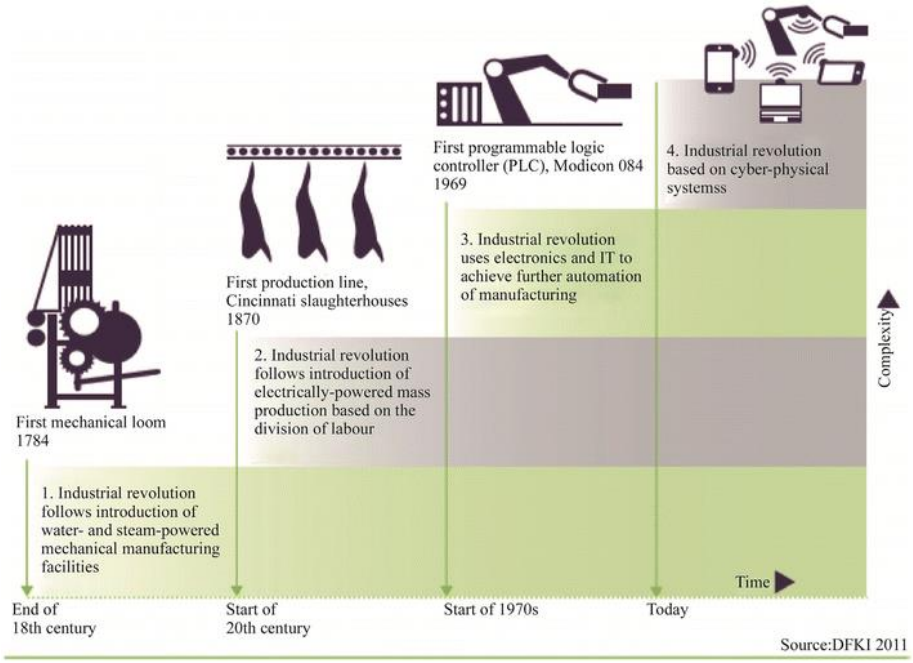

Figure 1: The four stages of Industrial Revolution (Kagermann, 2013, p. 13)

In the same way, for some years we have been witnessing relevant changes that for their velocity, breadth, depth and impact seem to identify a fourth industrial revolution[1]. However, contrary to the previous ones, this current paradigm shift is not only being observed as it occurs, but it has been somehow planned ex-ante[2]. In fact, the promising possibilities that appear for industrial development led to the rise of an innovative and future-looking concept known as Industry 4.0, that came to represent and fuel the new industrial revolution. Before focusing on the history and definition of Industry 4.0, the analysis will explore the main drivers behind the current paradigm shift. It is necessary to highlight that there is no agreement on the fact that Industry 4.0 and the Fourth Industrial Revolution are the same thing[3]: for example, Schwab believes that the Fourth Industrial Revolution is a wider concept. However, for the many features that they share, in this analysis they will be treated as the same thing. A common aspect of big industrial transitions, in general, is that they can all be explained by megatrends. The paragraphs that follow will illustrate the three drivers of the Fourth Industrial Revolution, that were identified in a report of the World Economic Forum: connectivity, intelligence and automation[4].

1.1.1 Drivers

Connectivity

Connectivity is a fundamental megatrend of the Fourth Industrial Revolution, as it entails the creation of new sophisticated models of collaboration and competition, facilitated by the rise of a borderless or boundaryless society. At the industrial level, connectivity is what shapes the new industrial developments, by appearing across all elements and processes of production[5]. The most obvious expression of connectivity is in the items of the factory, in which the physical and computational spheres are now fully intertwined, thanks to the development of sensors. This allows further connectivity, as all these items can be part of an internal network and exchange data and information across all phases of production, thanks to the Internet of Things. Finally, connectivity can also place the factory in an external network, that makes communication and interaction with suppliers,

1 Schwab., K. 2016
2 Lasi, H., Fettke, P., Kemper, H.G., et al. 2014
3 Schwab., K. 2016
4 World Economic Forum, 2019. However, the three megatrends were first identified by McKinsey in the 2018 edition of their annual survey on Digital Manufacturing.
5 Pereira, A. C., Romero, F., 2017.

customers and other operators easier and allows integrated management of the whole supply chain[6]. Connectivity is, therefore, the basis for networking. This concept has always been considered second-rate, compared to advanced technologies leading the way in the factory. However, networking through advanced connectivity is now seen as a priority and as a means to improve the structure of the firm and production of goods and services. Connectivity is fundamental in shaping the changes in our society, as it goes beyond the factory and reaches out to all levels of society. Nowadays connectivity is present in our daily lives through smartphones, social networks and instant messaging, turning into hyper-connectivity. This term was coined to describe "the availability of people for communication anywhere and anytime"[7] and it is one of the indirect effects of CMC (Computer Mediated Communication). The main technologies that underpin connectivity itself and the interest of factories in pursuing advanced connectivity solutions are 5G and Low Earth satellite orbits[8]. The former is an augmented wireless cellular connection, characterized by increased speed and availability. The latter consists of satellites that will grant internet connection even in the most remote areas of the earth. By increasing connectivity in different ways, these two technologies will contribute to the fulfilment of the prediction from CISCO systems, that forecasts that by 2022 28,5 billion devices will be connected in the Internet of Things[9].

Intelligence

In the context of the industrial revolution, the concept of intelligence incorporates robots, devices and machines that act intelligently, i.e. what commonly falls under the umbrella of AI (Artificial Intelligence). The revolutionary impact of these items is obvious from the speed at which they are developing and from their presence in daily life, that is tangible in smartphones, laptops, self-driving vehicles[10]. Regarding the pace of development, it is interesting to observe that simply employing AI in the factory is not enough to be competitive. In the book "The AI advantage"[11], three stages of AI usage are identified[12]. The first one is Assisted Intelligence, in which the data are processed by humans only with limited help from the machines. The second stage is called Augmented

6 Rojko, A., 2017.
7 Quan-Haase, A., Wellmann, B., 2005.
8 Deloitte, 2019, pp. 58-59.
9 Report available at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf
10 Schwab, K., 2016.
11 Davenport, T.H., 2018.
12 *Ibidem*.

Intelligence, as the machine can increase human knowledge and ability to process data. The final stage, the one factories should aim for, is Autonomous Intelligence. In this phase, like for connectivity, the ability of machines to understand and learn is granted by very advanced sensors and by the increased amount of data they can store and process and this allows them to perform increasingly difficult tasks, including advanced decision-making processes. As Schwab reports, in a survey of the World Economic Forum's Global Agenda Council on the Future of Software and Society, the respondents were asked to decide which phenomena according to them were likely to occur within 2025. A percentage equal to 42,5% believed that within that year, an AI machine would be found in a board of directors. In 2014, a venture capital firm gave an algorithm the possibility to vote in order to decide whether to invest or not in a company[13].

Finally, embracing this megatrend will also allow keeping pace with another major shift that is occurring in production dynamics, i.e. mass customization[14]. This entails that personalized goods and services are produced while maintaining the benefits of mass production. This process is also aided by AI, that is capable of segmenting customers by various criteria and adjusting the features of the product or service in order to make it personalized.

Automation

Automation is the performance of tasks with little or no human support. This element is the combination of connectivity and intelligence in the sense that, being all the machines interconnected and intelligent and therefore able to communicate, understand, learn and make decisions, they can very often substitute humans in the fulfilment of tasks. This megatrend is fundamental in the Fourth Industrial Revolution as it has a huge impact both on the industrial system and on human life, by reshaping the features and needs of the job market. At the industrial level, the automation of tasks in the factory improves the scale, speed and quality of production, implying that workers are prepared to perform different tasks, more specialized and complex and that new opportunities are created for them to reach this aim[15]. Giving workers the opportunity to reskill is fundamental as workers should never be totally replaced, as it is shown that AI and human workforce should complement each other. In the 2018 Deloitte Global Human Capital Trends report, it is

13 Schwab, K., 2016. p. 311.
14 *Ibidem*, p. 27.
15 Pereira, A. C., Romero, F., 2017.

observed that often the implementation of automated processes is justified by the need of workers to discard the tasks that can be performed automatically, in order to focus on the relationship with clients. The report also shows that the demand for human skills, such as creativity and critical thinking, is predicted to increase dramatically[16]. Finally, according to the aforementioned report of the World Economic Forum, only 5% of jobs are fully automatable, while most of the jobs can be automatized by 30%, which means that more and more often workers, other than reskilling, will have the opportunity of performing tasks that are different and less monotonous[17].

1.1.2 Definition and first developments

The first time the concept of Industry 4.0 appears is in a communication made by Dr. Henning Kagermann, Dr. Wolf-Dieter Lukas and Dr. Wolfgang Wahlster at the 2011 edition of the Hannover Fair[18]. In the communication, after acknowledging the shifts that are characterizing the latest industrial developments, Industry 4.0 is presented as a project aimed to invest in the German industrial system in order to make it able to compete at a global level.

The German government shows its support for the project right away, by including it in its "High-Tech Strategy 2020 for Germany". Meanwhile, the Industrie 4.0 Working Group is constituted, with representatives both from the research and industrial community, with the aim of researching the needs of industry and the key areas for the implementation of the project. The results of the Working Group are presented in a final report "Recommendations for implementing the strategic initiative INDUSTRIE 4.0", published on April 2013[19]. In this paper, the authors analyse the huge potential held by the project and the opportunities that it offers. These include the satisfaction of clients' requirements through customization, increased flexibility of production and, as a consequence, the rise of new business models. All of this is possible while responding to global challenges such as the pursuit of sustainability, through the continuous research of new materials and resources efficiency. Demographic changes will be addressed too, by

16 Deloitte Insights, 2018, p. 76.
17 World Economic Forum, 2019, p. 17.
18 Retrieved from https://www.ingenieur.de/technik/fachbereiche/produktion/industrie-40-mit-internet-dinge-weg-4-industriellen-revolution/ .
19 Kagermann, H., Wahlster, W., Helbig, J., 2013.

requiring new and more creative skills and by reaching a degree of flexibility in the workplace that allows the employees to find a good life-work balance.

In this significant document, it is also announced that the Industrie 4.0 Working Group will pass the torch of further implementation to the Industrie 4.0 Platform, founded by three important German professional associations, The Federal Association for Information Technology, Telecommunications and New Media (BITKOM), The German Machinery and Plant Engineering Association (VDMA) and The Electrical and Electronic Manufacturers' Association (ZVEI), thus granting the respect of a cross-sectoral approach.

However, neither in the 2011 communication nor in the 2013 report a formal definition of Industry 4.0 appears. The first formulation that accurately describes the concept is given in 2013 by GTAI (Germany Trade and Invest, the economic development agency of the Federal Government), in a report that explores the current state and future opportunities of the German industrial system[20]. The definition states as follows:

> "Smart industry or "INDUSTRIE 4.0" refers to the technological evolution from embedded systems to cyber-physical systems. Put simply, INDUSTRIE 4.0 represents the coming fourth industrial revolution on the way to an Internet of Things, Data and Services. Decentralized intelligence helps create intelligent object networking and independent process management, with the interaction of the real and virtual worlds representing a crucial new aspect of the manufacturing and production process. INDUSTRIE 4.0 represents a paradigm shift from "centralized" to "decentralized" production - made possible by technological advances which constitute a reversal of conventional production process logic. Simply put, this means that industrial production machinery no longer simply "processes" the product, but that the product communicates with the machinery to tell it exactly what to do."[21]

Thus, over the years, not only more definitions of the concept began to appear, but it also started receiving attention outside of Germany. In fact, in 2015 Industrie 4.0 makes its first appearance in a European context, in the Communication of the European Commission "A Digital Single Market Strategy for Europe"[22]. In this document, the European Commission acknowledges the speed and impact of the changes caused by the Internet and digital technologies, as well as the opportunities arising from this situation. In this light, the Commission announces a multi-annual strategy, aimed at the creation of a Digital Single Market, i.e. a market in which not only the free movement of goods, persons, services and capital is granted, but also the free access to online activities. In this document, Industry 4.0 appears as a term that generally describes the digitisation of

[20] GTAI, 2013.
[21] Ibidem, p. 6.
[22] European Commission, 2015.

manufacturing, that is one of the aims to reach in order to support the growth of the Digital Economy[23].

The interest of Europe in this concept keeps growing, as "Industry 4.0, Digitalisation for Productivity and Growth", an important briefing published in 2015 by the European Parliament shows[24].

The document is a more detailed excursus on how the European industrial system should exploit new technologies and as a consequence implement the Digital Single Market Strategy. The most commonly used definition of Industry 4.0 comes from this paper and it goes as follows:

> "Industry 4.0 is a term applied to a group of rapid transformations in the design, manufacture, operation and service of manufacturing systems and products. The 4.0 designation signifies that this is the world's fourth industrial revolution, the successor to three earlier industrial revolutions that caused quantum leaps in productivity and changed the lives of people throughout the world"[25].

The relevance of this document can be found in many aspects. TO begin with, it is the first document that is entirely dedicated to Industry 4.0. Secondly, it gives a clear outline of all the communications and initiatives that Europe promulgated and supported in order to implement the project and lists all the Member States that started engaging with it and their specific initiatives. Germany, from the invention of Industrie 4.0 to 2015, had already contributed €200 million to implement the project, while the other pioneers were mainly Italy, France and UK, that all initiated projects aimed at developing the Factory of the Future[26]. Finally, Industry 4.0 is a European concept.

The support for the project shown by the Member States paves the way for another initiative in 2016, called "Digitising European Industry"[27] (DEI).

In fact, whilst in this document the European Commission acknowledges the commitment and efforts shown by the Member States in exploiting the opportunities given by the digital technologies, it addresses the risks coming from the lack of a coordinated strategy. An excessive fragmentation bears many risks, such as the loss of investments, that may be directed towards other countries. For example, as the document reports, the investments made by European companies in R&D is only 40% compared to American companies[28]. Furthermore, only with a coordinated effort it will be possible to address

---

23 *Ibidem*, p. 15.
24 European Parliament, 2015.
25 Ibidem, p. 2.
26 Ibidem.
27 European Commission, 2016.
28 European Commission, 2016, pp. 5-6.

some of the weaknesses of the European digital industrial system, such as the need for standardisation and the convergence of sectors, areas and different types of enterprises. In particular, the gap between the digitisation of SMEs and larger companies could not be neglected anymore.

1.1.3 Where Europe stands now

The aforementioned document led to the launch, in 2017, of the European Platform of National Initiatives on Digitising Industry[29]. The platform is the main pillar of the Digitising European Industry strategy and it is aimed at boosting national Industry 4.0 related initiatives. This measure led to the creation of 15 initiatives all over Europe. After measures are proposed to reach aims, instruments for monitoring progress and accomplished objectives are needed. This is the task of the Digital Economy and Society Index[30] (DESI) (Figure 2) and the Digital Transformation Scoreboard (DTS)[31].

The first one is more synthetic, as it measures the performance both of Europe in general and of each European country, for what regards digitization in every aspect of society. The index is built on five sub-indicators: Connectivity, Human Capital, Use of Internet Services, Integration of Digital Technology and Digital Public Services. The 2018 report shows that, although all European countries grew in terms of digital performance, the leaders are Scandinavian countries, the Netherlands and the United Kingdom. The Member States that are lagging behind are instead Bulgaria, Romania and Greece. The rankings are also similar for what concerns the Integration of Digital Technology Index, the sub-indicator that analyses industries and businesses. The Integration of Digital Technology indicator is the one that analyses businesses in detail and it is, in turn, divided into two other sub-indexes, i.e. business digitisation and e-commerce. The best performing countries are Ireland, Netherlands, Belgium, Denmark and Finland.

Conversely, the Digital Transformation Scoreboard has a smaller scope and has a more detailed focus on the results of the European Platform of National Initiatives on Digitising Industry and Industry 4.0-related activities.

29 See https://ec.europa.eu/digital-single-market/en/pillars-digitising-european-industry-initiative .
30 European Commission, 2019.
31 European Union, 2018.

The fact that from 2016 so many measures were fuelled to support digital growth of the European industrial system is already a significant indicator and considered the short time range, it is understandable that many of the expected results have not been delivered yet[32].

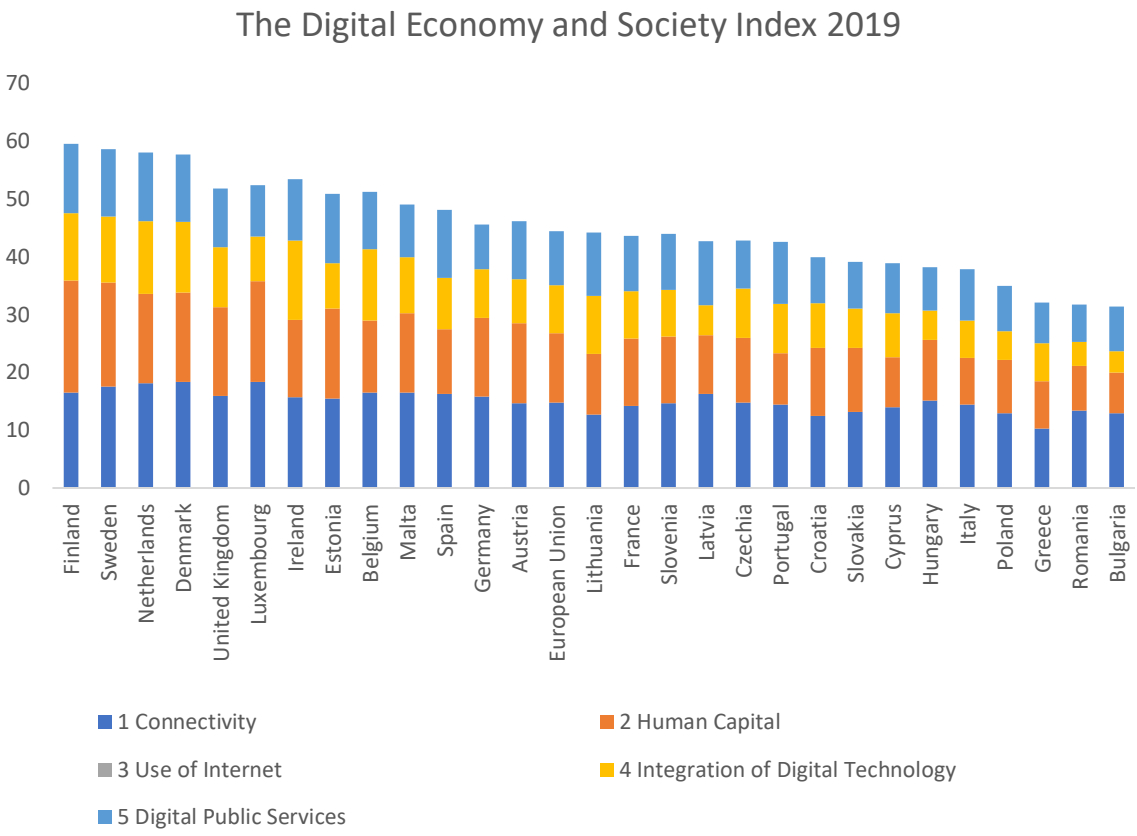

Figure 2: The Digital Economy and Society Index 2019 (author's elaboration on European Commission 2019)

However, it is clear that much of the great potential of digitisation still has to be unlocked. The DTS identifies nine fundamental digital technologies, i.e. Social Media, Big Data and Data Analytics, Cloud Technologies, Internet of Things, Mobile Services, Robotics and Automated Machinery, Cyber-security solutions, 3D Printing and Artificial Intelligence. Whilst almost 9 out of 10 companies believe that digital technologies are an opportunity, the rate of adoption is still very low. Of the interviewed companies, only 67% adopted one of these technologies, while only 35% adopted at least two[33]. The most

[32] European Commission, 2018, p. 11.
[33] Ibidem, p. 19.

adopted technologies of the last report (2018 edition) are Social Media, Big Data and Analytics and Cloud, with an adoption rate, respectively, of 31%, 24% and 23% (Figure 3).

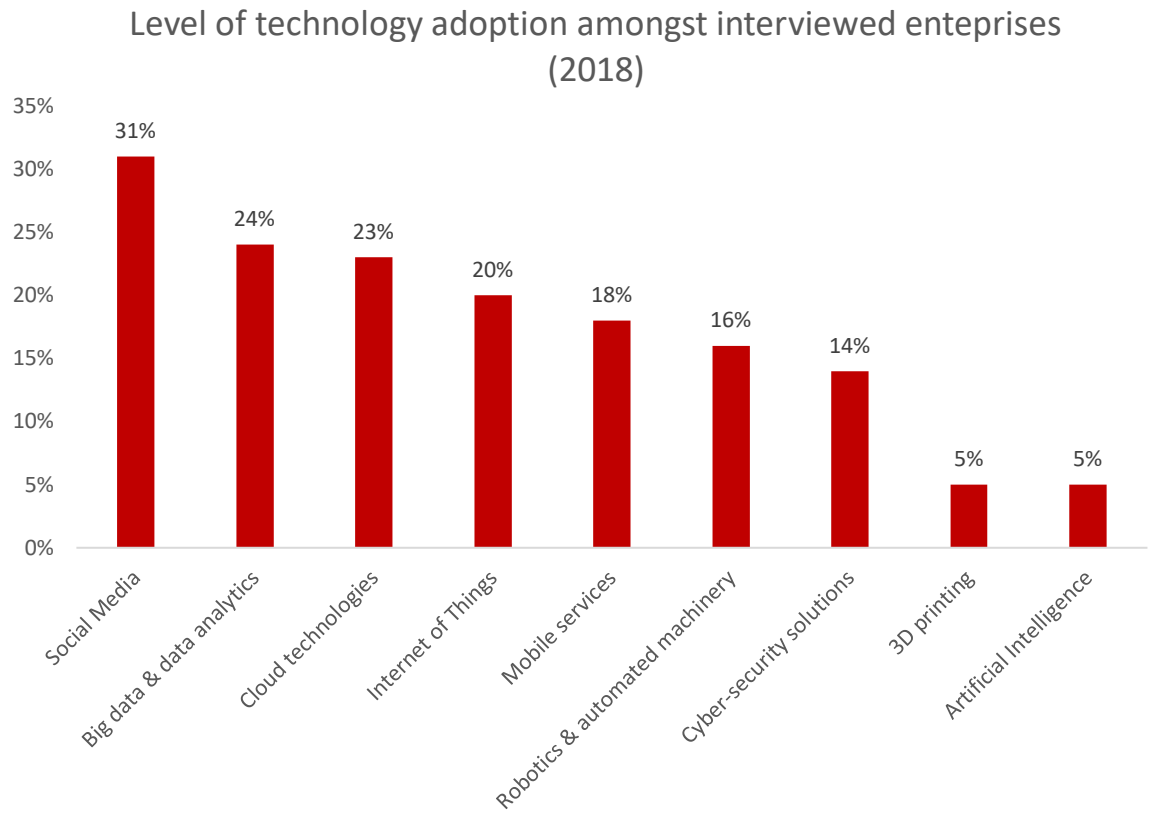

Figure 3: Level of technology adoption (author's elaboration from European Commission 2018)

Taking a closer look to the types of firms, the report shows that small and young firms are more likely to adopt at least one of the key nine technologies. In particular, 75% of firms that have less than 10 employees have adopted at least one technology and the more the number of employees grows, the more the percentage decreases: only 50% of firms with more than 250 employees adopted a key technology. In the same way, 75% of businesses that are between 0 and 2 years old are using at least one technology, while only 58% of firms that are 15 years old or more has adopted a technology.

In conclusion, even if in different ways, both reports show that, despite the fast growth of Industry 4.0, the path to fill the gaps between regions of Europe and different types of businesses is still long. However, one last insight shown of the DTS report shows that the

methodology used to understand whether the Industry 4.0 project is being implemented in a firm is to observe whether these 9 key technologies are being deployed. Therefore, one may think that these technologies are the features of Industry 4.0. Yet, defining them is much more complicated than it seems and at the same time, fundamental to better shape the context of the analysis and understand the research question. Thus, defining the characteristics of Industry 4.0 will be the first aim of the next paragraph.

1.2 The Components of Industry 4.0

1.2.1 A literature review

One necessary step to understand the concept of Industry 4.0 is to identify its components. As introduced in the previous chapter, this is not an easy task, as no homogeneous literature around the concept currently exists. A fundamental effort was done by Hermann, Pentek and Otto in their paper "Design Principles for Industrie 4.0 Scenarios: A Literature Review"[34]. However, they published the article in 2015 and its aim was mainly defining the concept of Industry 4.0 and its design principles. Thus, a new literature review will be presented, drawing on the methodology of Hermann, Pentek and Otto. It is necessary to write about the components of Industry 4.0 because, especially after the aforementioned work, much has been written about the definition of Industry 4.0 and, in general, the literature about the concept grew dramatically. This led to a fragmentation in the identification and definition of its features and components. In particular, it is possible to identify some keywords associated to Industry 4.0, i.e. the Smart Factory, the Internet of Things, Cyber-physical Systems (CPS) and Big Data, but there is a lack of agreement on how to systematise these concepts, making it difficult, in turn, to describe the relationship between them.

The starting point is the 2013 final report of the Industrie 4.0 Working Group[35], as it is a very relevant document in the Industry 4.0 literature. According to Kagermann, "Smart Factories are key features of Industry 4.0"[36]: this highlights the importance of this component right away. However, the author does not write about features or elements, as what he really stresses in the paper, is the need not to actually consider any aspect of

[34] Hermann, M., Pentek, T., Otto, B., 2015.
[35] Kagermann, H., Wahlster, W., Helbig, J., 2013.
[36] Ibidem, p. 19.

Industry 4.0 as isolated. Conversely, Cyber-Physical Systems are perfectly integrated through the Internet of Things, allowing the transformation of the whole value chain. The latter, as a consequence, will become smart itself and will be made of Smart Products, Smart Logistics, Smart Mobility, Smart Grids and Smart Buildings[37]. In a way, the Smart Factory is both the physical place where all this happens and an intangible concept that describes Industry 4.0 as the rise of a new manufacturing environment. It is interesting to notice that the topic of Big Data does not have a central position in the paper and it is not seen as a fundament of Industry 4.0, rather being an accessory technology. Finally, this document is relevant not only because it identifies some components of the Smart Factory but also because it describes one of its main objectives, i.e. integration. According to Kagermann, the implementation of the Smart Factory will contribute to reaching three degrees of integration, vertical, through networked manufacturing systems, horizontal, through value networks and end-to-end engineering, across the entire valuechain[38]. Vertical integration is achieved when all the subsystems, both physical and informational of the factory, are integrated to obtain a flexible structure[39]; horizontal integration consists of successfully inserting the factory in a bigger network of factories that can easily communicate and interact; end-to-end engineering integration entails that all the activities of the value creation process are integrated in a way to create a fixed model that can be used at every step and for every product or service produced[40].

Continuing in chronological order, there is an important paper published in 2014 by Lasi, Kemper and Fettke[41]. In this document, the authors aim at identifying possible developments of Industry 4.0 and propose an original way to systematise the driving forces of the fourth industrial revolution, based on application-pulls and technology-pushes. These notions are the two directions in which the development of Industry 4.0 is going. In particular, "on the one hand there is a huge application-pull, which induces a remarkable need for changes due to changing operative framework conditions. […] On the other hand, there is an exceptional technology-push in industrial practice"[42]. Regarding the principal aspects of Industry 4.0, the authors describe them as fundamental concepts. These include the Smart Factory, Cyber-physical systems, self-organization,

37 Ibidem.
38 Ibidem, p. 6.
39 Pereira, A. C., Romero, F., 2017.
40 Ibidem.
41 Lasi, H., Kemper, P., Fettke, H., 2014.
42 Ibidem, p. 239.

new systems in distribution and procurement, a new system in the development of products and services, adaptation to human needs and Corporate Social Responsibility. The centrality of the Smart Factory is evident in this document too, also because all the other dimensions listed by the authors can refer to a subfield of the Smart Factory. However, individual space is dedicated to aspects that are enabled by the Smart Factory, such as the development of products and services, while other enabling concepts are not considered central, such as the Internet of Things and Big Data.

The next paper is "Industrie 4.0: Enabling Technologies" from Wan, Cai and Zhou[43]. Similarly, these three authors show an original approach as they write about themes and enabling technologies of Industry 4.0. The two themes are realizing the Smart Factory and realizing intelligent production and management. Once again, the Smart Factory is the most relevant component, followed by Cyber-physical Systems and Internet of Things that are its enabling technologies. In particular, according to the authors, Cyber-physical systems are the basis of both themes. The intelligent factory combines them with IoT to achieve the perfect integration of the virtual and physical world. The second theme's aim is "to fabricate products that integrate the informatization and industrialization"[44]. Finally, in this paper more attention is given to the aspect of Big Data. According to the authors, the increased importance of data is given by the combined development of Cyber-physical systems and intelligent manufacturing, that require more and more cheap and secure data. The overall relationship between the two themes and the enabling technologies is described as follows: "Actually, intelligent factories are new intelligent manufacturing system that contains future advanced manufacturing technology based on application and arrangement of Big Data management"[45].

Another paper aimed at comprehensively analysing Industry 4.0 is "A review of the meanings and the implications of the Industry 4.0 concept", published in 2017 by Pereira and Romero[46]. In this essay, a precise definition of the Smart Factory or its identification as an individual element lack. However, the authors write:

"Industry 4.0, which may eventually represent a fourth industrial revolution, is a complex technological system that has been widely discussed and researched, having a great influence in the industrial sector, since it introduces relevant advancements that are related with smart and future factories. This emerging Industry 4.0 concept is an umbrella term for a new industrial paradigm that embraces a set of future

43 Wan, J., Cai, H., Zhou, K., 2015.
44 Ibidem, p. 137.
45 Ibidem, p. 138.
46 Pereira, A. C., Romero, F., 2017.

industrial developments regarding Cyber-Physical Systems (CPS), Internet of Things (IoT), Internet of Services (IoS), Robotics, Big Data, Cloud Manufacturing and Augmented Reality."[47]

Therefore, the importance of the Smart Factory is still evident in the centrality of the new intelligent production system, that the abovementioned technologies allow. Also in this paper, Big Data is recognised as an individual main component.

The last document that was analysed is "Industry 4.0 – A Glimpse" by Vaydia, Ambad and Bhosle and aims at identifying the challenges associated with the carry-out of the Industry 4.0 project and its future trends[48]. In this document, the focus is on Smart Manufacturing, rather than on the Smart Factory, which together with Internet of Things and Industrial Internet of Things form the main drivers of Industry 4.0. Smart Manufacturing is the main aim of Industry 4.0, which is implemented thanks to its main associated technologies, that are defined as pillars. They are Big Data and Analytics, Autonomous Robots, Simulation, System Integration, the Industrial Internet of Things, Cybersecurity and cyber-physical systems, the Cloud, Additive Manufacturing and Augmented Reality[49].

As anticipated at the beginning of the paragraph, although much has been written about Industry 4.0, there is neither agreement on what its components are, nor on how they interact. However, some principles can be deducted: the Smart Factory is a core element, as it can represent both physically and ideally what Industry 4.0 tries to implement. Cyber-physical Systems and the Internet of Things can be defined as technology enablers. In fact, without them the Smart Factory could not exist and, as a consequence, Industry 4.0 could not be carried out. The role of Big Data is as important as the one of Cyber-Physical Systems and the Internet of Things. It is interesting to notice how this became clearer later, by the increasing centrality attributed to the concept in the analysed literature. Finally, all the other technologies are important but they are still secondary, as they were implemented thanks to the dramatic development of CPS, IoT and Big Data and their combined use in the Smart Factory.

In conclusion, a definition of Cyber-Physical Systems and the Internet of Things will be provided in the following lines, while a more detailed description will be carried out for the Smart Factory and Big Data, due to their importance in the analysis.

---

47 Ibidem, p. 1207.
48 Vaidya, S., Ambad, P., Bhosle, S., 2018.
49 Ibidem.

Cyber-Physical Systems are machines that, due to the integration of ICT elements, can perform a variety of tasks autonomously, such as managing industrial operations and process data. CPS are the third stage in the evolution of physical-virtual integration, as reported by Hermann, Pentek and Otto[50]. First-generation CPS were only identifiable, through RFID technology; second generation ones had sensors that allowed them to perform a limited number of tasks; third-generation ones, thanks to their ability to process data, can learn, remember and join together in a network. CPS ensure that the factory becomes smart, by allowing it to become decentralized and virtualized, especially as they keep evolving into even more advanced technologies, such as Digital Twin[51]. More on these topics will be examined in the next paragraph.

When Cyber-Physical Systems join together in a network, they form the Internet of Things, that can be defined as when "'things' and 'objects', such as RFID, sensors, actuators, mobile phones, which, through unique addressing schemas, (...) interact with each other and cooperate with their neighboring 'smart' components, to reach common goals"[52]. Of course, things and objects can be machines and plants and it is by connecting such devices that the Internet of Things brought such dramatic changes to manufacturing as we knew it.

As a consequence, it is through the integration of these two fundamental technologies that the Smart Factory can be implemented. In the next paragraph, the qualities that result from the combination of the above-mentioned technologies in the manufacturing environment will be outlined, making it possible to identify and define the Smart Factory.

1.2.2 The Smart Factory

The Smart Factory is the key factor of Industry 4.0 and it was defined by Hermann, Pentek and Otto as "a factory where CPS communicate over the IoT and assist people and machines in the execution of their tasks"[53]. In order to describe the Smart Factory accurately, it is useful to go through its features. They can both identify the factories that have de facto embraced the new technological and organizational developments, or describe the areas in which a firm should invest to be competitive nowadays. This is the

50 Hermann, M., Pentek, T., Otto, B., 2015.
51 Qi, Q., Tao, F., 2017.
52 Giusto, Lera, Morabito, & Atzori, 2010, p. V.
53 Hermann, M., Pentek, T., Otto, B., 2015, p. 10.

approach of Mabkhot et al., who identify the six "requirements" of the Smart Factory[54]: modularity, interoperability, decentralization, virtualization, service orientation and responsiveness.

Modularity depends on how independent the components of a system are. When they are tied loosely, it means that they can be reassembled easily and quickly and modularity is achieved. This feature can be applied both to products and to organizations. When a product is designed in a modular way, it means that its components rely on standardized components interfaces, that when reassembled and integrated with the other components allow a certain degree of variation in the product. When this applies to the components of an organization rather than of a product, it means the parts of the production line can be recombined in any way and the factory achieved modularity[55].

Interoperability refers again to the components of the factory and to their capability to communicate and cooperate, exchanging information and data. It is a very important feature as it is the one that allows two out of the three degrees of integration that, as previously explained, are fundamental for implementing Industry 4.0[56]. The achievement of this ability can be explained by a shift from a manufacturing model based on the traditional automation pyramid to the automation network. The former is made of five levels. Starting from the top, there is the Enterprise Resource Planning (ERP), a tool which refers to a variety of management activities. Then the Manufacturing Execution System (MES) follows, that manages production from scheduling to maintenance operations, to resource allocation. The third and fourth level aims at process control, based on Supervisory Control and Data Acquisition (SCADA) and the physical controllers known as Programmable Logic Controllers (PLCs). Finally, the last level is the production level[57] (Figure 4). This model started showing flexibility issues, caused by the lack of interaction and exchange between non-adjacent levels[58]. The introduction of smart devices and cloud computing solved these problems, transforming the factory in a non-hierarchical vertically integrated environment, and hence it achieved interoperability. When this concept expands to communication and interaction in a wider

54 Mabkhot, M., Al-Ahmari, A. Salah, B., Alkhalefah, H., 2018.
55 Sanchez, M., Mahoney, J.T., 1996.
56 Horizontal Integration, Vertical Integration and End-to-End integration, as from Kagermann et. Al. 2013. Zeid, A., Sundaram, S., Moghaddam, M., Sagar, K., Marion, T., 2019.
57 Rojko, A., 2017.
58 Zeid, A., Sundaram, S., Moghaddam, M., Sagar, K., Marion, T., 2019.

network, i.e. the one of different Business Units or different factories, integration becomes horizontal too.

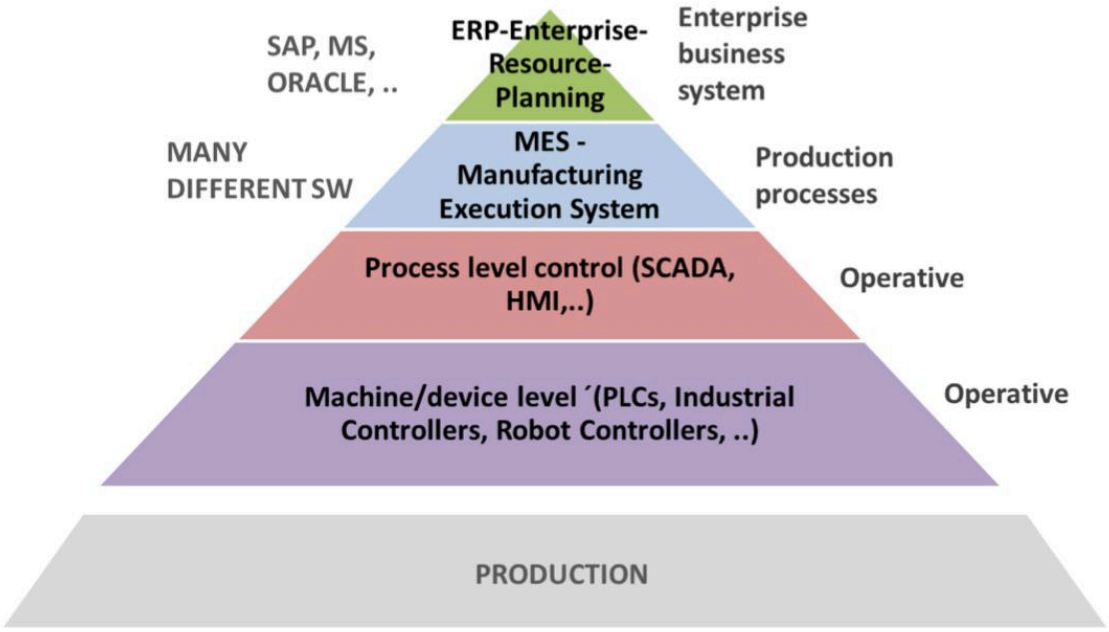

Figure 4: Automation Pyramid (Rojko,A.,2017 p. 83)

Decentralization is strictly correlated with interoperability, as a more integrated system also entails that components can decide independently. This feature is allowed by CPS, therefore it is a fundamental characteristic of the Smart Factory, as CPS are its main pillars. However, decentralization does not finish with CPS but grows in scope and meaning thanks to other innovative technologies, such as additive manufacturing, that is commonly considered one of the main innovations of Industry 4.0 and the Smart Factory. Additive Manufacturing, also known as 3D printing, consists in the creation of products, thanks to a machine that automatically spouts layers of material, following a structure usually created with computer-aided design. If this technology keeps developing at this fast pace, decentralization will be brought to a whole new level. Products will be more often produced in the country where they are sold, firms will be split into many highly independent plants and new operators will enter the market, as the technology is becoming less and less difficult to use[59].

[59] Avner, B., Siemsen, E., 2017.

Virtualization refers to the existence of a virtual version of the components of the factory, that allow the simulation and monitoring of its processes. Like with decentralization, CPS are the first enablers of virtualization, as they are items embedded with a computational sphere and therefore they allow the integration of the physical and the virtual world. However, also CPS keep evolving and with them, the degree of virtualization of the factory. Another very recent technology of the Smart Factory, that is developing at a very fast pace, is the Digital Twin. This concept allows the virtualization of the whole factory, from material and tools to the manufacturing process[60].

Service-orientation can refer to two different concepts. In fact, Makbhot et al. describe it as "the idea that manufacturing industries will shift from selling products to selling products and services"[61]. In this case, the feature is a trend that develops as a consequence of demand shifts. As products reached a common and very high level of quality, the way to be competitive is to sell them with a service. According to other authors, such as Bauer, Stock and Bauernhansl, service orientation is rather a technical shift in manufacturing, that is related to the obsolescence of the traditional automation pyramid[62]. Manufacturing IT changes result not only in increased interoperability, but also in the division of software functionalities into services and apps. As a consequence, manufacturing IT is now "also indicated as Everything as a Service (XaaS), a paradigm, which originates from the three main cloud computing service layers Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS)"[63].

Finally, responsiveness is the ability to adapt to changes and it is the consequence of so-called Reconfigurable Manufacturing, that should be the manufacturing model employed in the Smart Factory. The concept is the last stage of an evolution that started with the invention of the assembly line by Henry Ford. In this production process, the machines used were able to perform one task only in a very productive and cost-efficient way, i.e. the production lines were each dedicated to building a different piece of the car. Around the end of the past century, a new manufacturing process replaced production lines, thanks to the development of Numerical Control and Computer Numerical Control, allowing the creation of more than one component of a product. However, this system, called Flexible Manufacturing System (FMS) was not able to respond quickly enough to

60 Qi, Q., Tao, F., 2018.
61 Mabkhot, M., Al-Ahmari, A. Salah, B., Alkhalefah, H., 2018, p. 6.
62 Bauer, D., Stock, D., Bauernhansl, T., 2017
63 Ibidem, p. 199.

the challenges arising from the transportation powertrain industry. This led to the rise of Reconfigurable Manufacturing, as a system that allows firms to be cost-effective and responsive.[64]

1.2.3 Challenges of the Smart Factory

The features outlined in the previous paragraphs are those that characterise the Smart Factory. Although they can be considered requirements too, because factories that do not undergo all these changes will probably struggle to be competitive, there are some downsides too. The combination of the above-mentioned features will surely result in a more dynamic, flexible and competitive environment; however, this will also pose significant challenges that the entrepreneurs have to be prepared for. These include standardization, availability of the IT structure, availability of fast internet, non-technological risks and information security[65].

Standardization is a challenge mainly associated with interoperability and modularity. In fact, to allow that the components of the factory are mixable and that they communicate and interact, the IT systems of the factory have to be connected. Standardization would make this task less difficult, thus a frequent solution is to design and adopt a common architecture for Industry 4.0. The most famous one is called Reference Architectural Model Industry 4.0 (RAMI 4.0) and it was presented at the 2015 edition of the Hanover Fair. RAMI 4.0 is a three-dimensional model that shows, on the first axis the life-cycle and value stream of a product, on the second axis the hierarchical, i.e. the functional classification of a "situation" in the Smart Factory[66]. The last axis is made of layers that allow the description of both products and processes. After this model, many other solutions have been proposed, as a response to the increased need for standardisation. However, acknowledging the importance of common models is not enough and the path toward interoperability and modularity is still long, as many of the models proposed are still at an initial phase of implementation[67] (Figure 5).

[64] Rojko, A., 2017.
[65] Herrman, F., 2018.
[66] Ibidem.
[67] Ibidem

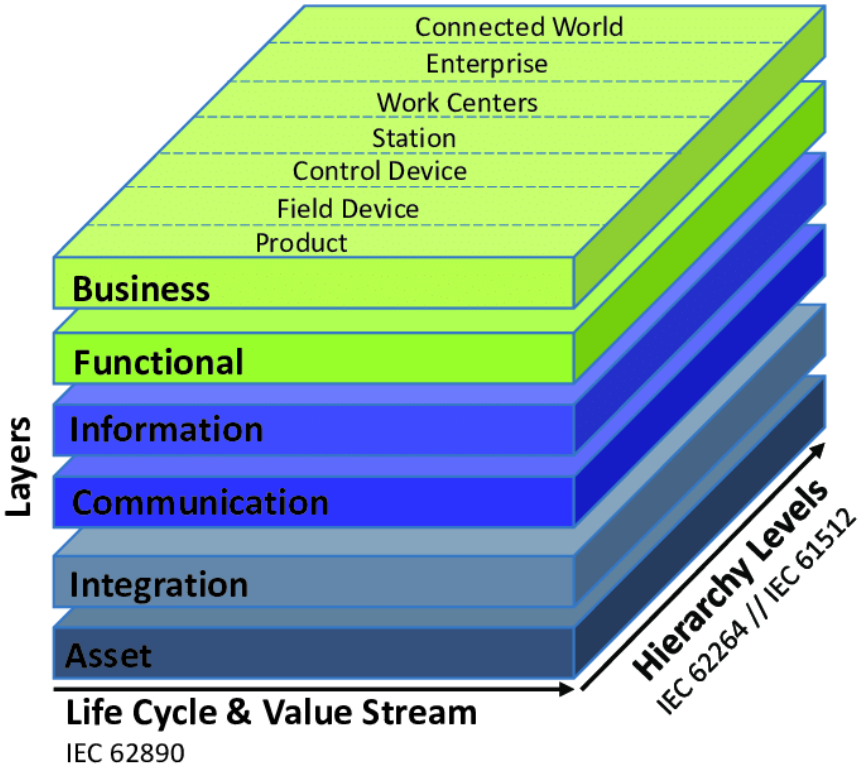

Figure 5: RAMI 4.0 model (Herrmann, F., 2018, p. 7)

The availability of the IT structure is fundamental in a Smart Factory for many different reasons. In fact, not only items and processes have to be connected in a network, but this network has to be modern and non-hierarchical. This aim is associated with the above-mentioned switch from the traditional automation pyramid. Being willing to reach a new degree of integration is not enough to reach a distributed structure, as the switch goes hand in hand with an IT structure that is non-hierarchical either. This is difficult as, normally, each layer of the pyramid has its own IT system, and all the components are in turn produced in different ages and firms, making the achievement of a common IT structure difficult and expensive[68].

To face all these challenges, it is also necessary to have a fast internet connection, that allows the Cyber-Physical Systems to be always interconnected in the network they form, without risking interruptions. Broadband is a very important aim in European Union at the moment, as many different objectives were outlined regarding this topic in the Digital Agenda for Europe and then in the communication "Gigabit society for 2025". In particular, the Digital Agenda's broadband-related objectives were i) to bring basic

[68] Ibidem.

broadband coverage to all European households ii) to bring fast broadband coverage to all European households by 2020 iii) to bring ultra-fast broadband to at least 50% of European households. Although all Member States made it to improve the availability of broadband for their citizens, a final report on the implementation of the Digital Agenda shows that the 2020 aims will not be met[69].

The non-technological risks associated with the Smart Factory are complexity, organizational risks and financial risks[70]. The transformation of the factory into an integrated, flexible and automated network leads to increased complexity of the system. That is why it is so important that nowadays' workforce is sufficiently skilled. The more the workforce is experienced, the more easily complex systems can be run and simplified. By cooperating to make this happen, also specialists' networks could be formed and work together to make European products the most competitive in the market. However, achieving the up-skilling of industrial workers is no easy task, in fact, when referring to organizational risks the main issue is related to employment. If on the one hand it gets clearer day by day that machines will not substitute men in the factory, on the other hand, employees will struggle to be employed if lacking specialization and skills. This has a relevant impact on the managerial level too, as it will have to propel most of the change, from the factory's digitalization processes to the design of new job profiles[71]. Financial risks have to be taken into account too. The implementation of the Smart Factory is still very expensive and both national and supranational authorities, as well as companies themselves, have to deal with the funding necessities of the new industrial system[72].

Finally, the last risk of the Smart Factory is information security. This topic can be divided into two areas: the first one refers to the safety against disruption of the operations and the other refers to the protection of personal data. The former is related to the risks that arise from the interconnectedness of the elements of the factory among each other and to the Internet of Things. When all the supply chain is aided by an advanced IT system that usually is situated on a cloud, this makes the whole production process exposed to the threats of hacking and sabotage. The protection of personal data is a tricky topic in the Smart Factory, because very often operators in these environments think that the only informational risks are those related to production, sales and supply-chain related data.

69 European Court of Auditors, 2018.
70 Herrman, F., 2018.
71 Pereira, A. C., Romero, F., 2017.
72 Herrman, F., 2018.

This is far from being true, as the features of the Smart Factory themselves, such as the interdependency of all its elements, entails the production of a great amount of personal data too. The protection of the latter in the context of the Smart Factory is the core of this analysis. However, beforehand it will be necessary to examine the role of data in general in this period, as well as their characteristics and classification. This will be the assignment of the next chapter.

2. Adjusting Data Protection to the Smart Factory

Big Data is one of the buzzwords of the fourth industrial revolution, as it is collected, analysed and applied in many fields. Thus, apart from a set of knowledge around Big Data in general, other implications of their characteristics, usage and protection may differ from field to field of application. In fact, the aim of Chapter 1 was to identify the context and scope of this analysis, i.e. the Smart Factory. However, before understanding how data are and should be regulated in the context of the Smart Factory, it is necessary to get to know the topic of data better. Therefore, this chapter will first define big data, what they are, how they are classified. Then, the focus will narrow down to how they are used or misused in the Smart Factory. Finally, a history of data regulation will be outlined in the last paragraph.

2.1 Big Data

2.1.1 A definition

As for Industry 4.0, many definitions were given of the concept of Big Data. Gartner, world leader for consulting and research in IT, defined it in its IT glossary as

"high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation"[73].

As it appears from this definition, the features that define big data are their Volume, Velocity and Variety. These concepts were first elaborated by Laney, who described the great changes that were affecting data and information[74]. In fact, it is necessary to point out that data and data analysis have existed for a long time, while what is changing is their quantity and availability. They became Big Data, when Volume, Velocity and Variety started increasing dramatically, as it happened in the last years.

Volume refers to the quantity of data that is collected and available. Estimating the precise amount of data is a very difficult task, however there is a general agreement on the fact that the trend of its growth is exponential[75]. In 2016 the first zettabyte of collective traffic on the Internet was reached, meaning that 10^{21} bytes of data were created[76]. As a consequence, the famous Moore's Law, that states that every two years the number of

[73] https://www.gartner.com/it-glossary/big-data
[74] Laney, D., 2001.
[75] AGCOM, 2018 p. 3.
[76] According to AGCOM (2018) this equals the time legth of 125 billions of DVDs.

chips put in an integrated circuit doubles, was overcome. According to many sources, the next threshold will be reached in 2025, with 175 zettabytes[77].

Velocity refers to more than one concept. The first one is the speed at which data are created and collected, the second refers to the speed of processing them. Both of these quantities have increased. In particular, business environments can now benefit from real-time processing, as this allows a very quick decision-making process. The responsiveness feature of the Smart Factory, described in the first chapter, refers to this ability too, that of course, is acquired together with a flexible business model and very advanced software[78]. Finally, velocity is also strictly related to volume, as it sheds new light on its dramatic growth. Whilst it took very long to reach one zettabyte, only from 2018 to 2025, this amount will have increased by more than 500%[79]. (Figure 6)

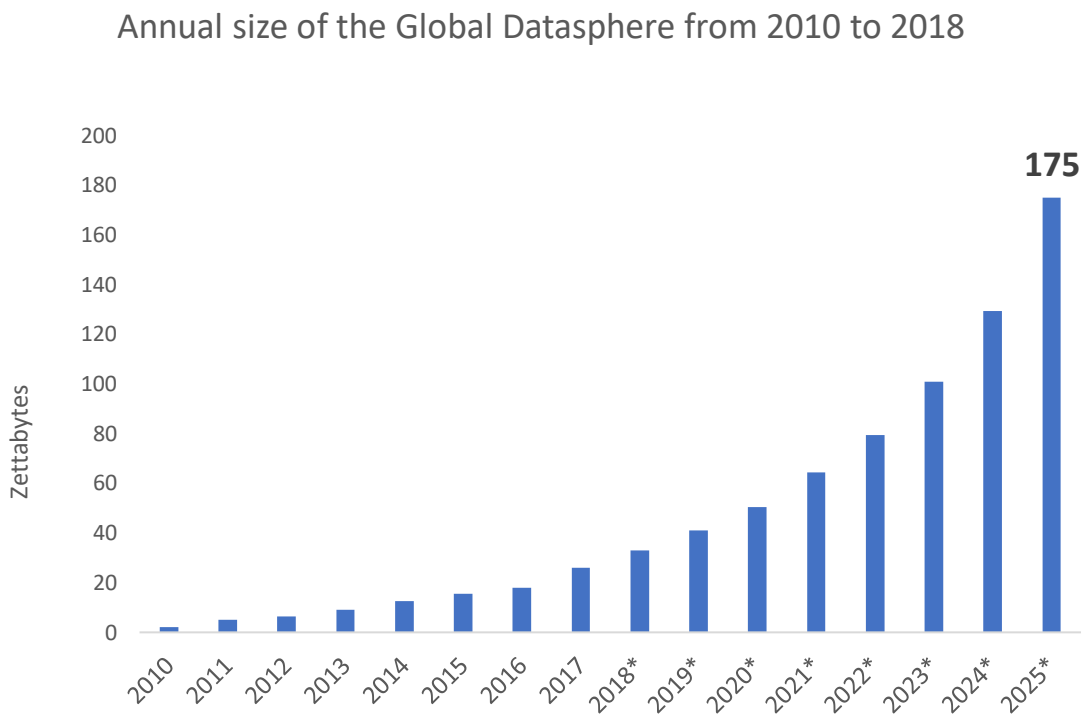

Figure 6: Annual size of the Global Datasphere (author's elaboration on Reinsel, D., Gantz, J., Rydning, J., 2018 p. 5)

77 Reinsel, D., Gantz, J., Rydning, J., 2018 p. 5
78 AGCOM, 2018, p. 9.
79 Reinsel, D., Gantz, J., Rydning, J., 2018 p. 5

Variety, as originally defined by Laney, refers to differences in data formats, structures and semantics[80]. The increase of this variable mainly depends on the switch from the prevalence of structured data to unstructured ones, that require advanced processes and technologies to be converted into actual information[81]. However, more on data classifications will be said in the next paragraphs.

Although all scholars have endorsed the definition of Big Data through these three characteristics, the research on this topic kept growing and many other "Vs" were added and counting all the features mentioned in the literature, the result would be 42 Vs. However, there is another definition that relies on the so-called 10 Vs, selected by Babiceanu and Seker from existing literature[82]. This set is especially relevant as it focuses on the engineering viewpoint that, according to the authors, gives precious insights regarding the use of Big Data in manufacturing. The additional seven Vs are:

Value: this feature refers to the purpose of data. It is a very interesting variable as it is believed that the more data are created, the less value each data has. This is also related to data exhaust, that results from our so-called online footprint[83]. However, it is interesting to notice that nowadays, even such data acquired great importance, as it is re-used to discern further information about the users[84].

Veracity validation and verification: they refer to the trustworthiness of data, which is fundamental for every business that relies on Big Data. In fact, according to a recent survey of Accenture[85], most executives responded that their organizations base the most critical decisions on data without verifying their accuracy. To avoid the vulnerabilities resulting from such behaviour, data intelligence should be carried out, in order to verify provenance, context and integrity[86].

Vision: this feature refers to the capability of discerning the role of data in a certain project or activity.

Volatility: because of the increased volume and velocity of data generation, it is necessary to determine carefully for how long a set of data can be kept and used to make decisions before it is considered too obsolete. And when this happens, new data to substitute old data should be created.

---

80 Laney, D., 2001, p.2.
81 AGCOM, 2018, p. 9.
82 Babiceanu R., Seker R., 2016.
83 Laney, D., 2001, p. 1.
84 AGCOM, 2018, p. 5.
85 Accenture, 2018.
86 Ibidem.

Variability: generated data has a level of uncertainty or impreciseness; this feature addresses aspects such as data inconsistency, incompleteness, ambiguities, latency, deception and approximations.

Finally, although these features give an insight into the meaning and reach of this phenomenon, another very important point of Big Data is that they belong to the same continuum of Small Data[87]. This is especially important for two reasons. Firstly, it means that companies do not have to deal with something new, but they rather have to gradually adjust to an increasing magnitude. Secondly, acknowledging that Big and Small data are on the same spectrum has to stimulate businesses never to forget to review all the data that are available to them. In fact, although most of the new data generated are unstructured, combined with transactional ones they provide the most useful information for businesses[88].

2.1.2 Types of data

As previously mentioned, one of the characteristics of Big Data is that their variety increased dramatically, leading to the existence of many different types of data. Classifying them is very important, so that they can be associated with a determined pattern. Classification can happen along many different criteria. Eight main lines were identified for classifying Big Data, i.e. the processing method, the analysis type, frequency, consumers, type, hardware, content, and sources[89].

Regarding the analysis type, it can be real-time and batch. A batch analysis type consists in making a determined and limited amount of data go through the phases of analysis, that are implemented by separate supports. As the amount of data grew, also the demand for a faster analysis type did, thus real-time analysis started being implemented, by putting data in a continuum of input, process, output. The demand for such type of analysis is obviously increasing, especially considering the demand of organization for tools that allow them to make decisions rapidly[90].

---

87 Jaap, B., Van Doorn, M., Duivestein, S., Van Manen, T., Van Ommeren, E., 2012

88 Ibidem.

89 Sangeetha, S., Sreeja, A.K., 2015. However, these criteria were first found in an article published by IBM in 2013. Retrieved from https://developer.ibm.com/articles/bd-archpatterns1/ .

90 Ibidem.

Processing data is a fundamental step in the framework of data usage in an organization and more than one method can be identified. They are mainly divided into analytics, predictive analysis, ad-hoc query reporting and miscellaneous[91]. Usually, the choice among these techniques varies according to the business. Analytics can in turn be divided into many other processes and it is especially useful for unstructured data: in fact, some techniques are text analysis, video analysis and audio analysis, that extract information from unstructured text, video and audio data. One technique that acquires increasing importance day by day is social media analytics, especially because of its application in marketing. However, from social media it is possible to extract data that are relevant for psychological, anthropological, sociological analysis and many other fields[92]. This technique relies on both structured and unstructured data. Predictive analysis includes other techniques too, but it mainly refers to the process of forecasting possible future outcomes based on historical and current data[93]. This processing method is mainly based on statistics, that are used to predict future outcomes. Like social media analysis, it can be applied to many fields. The third processing methodology is ad-hoc query. A query is a request for data extraction from a database. Ad hoc query refers to a situation in which data is extracted and processed only when a specific need generates the request. Finally, all these methodologies have their advantages and disadvantages, thus many organizations decide to rather use a combination of them.

The data frequency depends on the availability of the data feed, that is the mechanism that allows the reception of data from their sources. The feeds' availability can range from a monthly to a per-second basis. The main frequencies are on-demand, continuous, real-time and time series[94].

Data consumers are those who actually use the processed data and they can be mainly humans and business processes[95].

Data types can be metadata, transactional data, historical data and masterdata. Metadata are commonly described as data about data. In fact, a very common example of metadata is digital libraries, in which the metadata constitute all the information associated to a certain file, such as the title, the author, the ISBN etc.[96]. Transactional data refer to the

91 Sangeetha, S., Sreeja, A.K., 2015.
92 Gandomi, A., Haider, M., 2015, p. 142.
93 Ibidem, p. 143.
94 Sangeetha, S., Sreeja, A.K., 2015.
95 Ibidem.
96 Clobridge, A., 2010, p. 85.

data acquired thanks to a transaction, such as the purchase of an item. This is the type of data that experienced the most dramatic growth, as by now it includes not only traditional transactional data, but also all the information deriving from sensors, devices, social media and GPSs[97]. Masterdata are similar to transactional data, as they refer to transactions too, but they are less unique as they can identify more than one transaction[98]. Finally, historical data are the ones that are mainly used for predictive analysis as they are the record of something that existed or happened in the past.

The hardware refers to "the type of hardware on which the big data solution will be implemented"[99], that can be either commodity or state of the art. The former is a very inexpensive hardware that can usually run Windows, Linux and MS-DOS without an additional appliance, while the latter represents in general a hardware that is in its state of the art, i.e. in the stage of its most recent development.

The content type is the most famous criterion to classify data and it includes structured, unstructured and semi-structured data. Structured data are data that are already or can easily be inserted in a database. For this reason, also managing them and processing them is a straightforward task, as well as the extraction of value. Structured data almost identify with what is commonly intended by small data and in fact now they only represent 20% of the data existing in the world[100]. The remaining 80% is made of unstructured data, that refer to "data objects whose contents are not organized into arrays of attributes or values"[101]. Most of this data is produced by humans and it is shaped in text. Of course, the extraction of information and value from this data is more difficult, as well as the storage and management in general. Data mining and other advanced technologies are being developed in order to bring the form of these objects towards a more structured shape. This degree could represent semi-structured data, that are data that do not reside in a structured set of rows and columns but have some organizational features that make their analysis easier.

Finally, the last classification criterion is the data source. Big Data can be machine-generated and human-generated. The former refers to when data is the result of a computer process or application and in general, when it is created without any interference from human beings. The latter consists of all the files generated by humans

97 van der Lans, R., 2012, p. 264.
98 Reeve, A., 2015.
99 Sangeetha, S., Sreeja, A.K., 2015, p. 3270
100 AGCOM, 2018.
101 Berman, J.J., 2018, p. 2.

as they interact with digital and online services[102]. The topic of data origin is very important when dealing with personal data, as both the lines between personal and non-personal data and between machine-generated data and human data are getting blurred. For what concerns the latter, it may seem obvious that personal data are human-generated, as in machine-generated data there should not be any interference from people. However, with the technological advances including sensors, AI, Cyber-Physical Systems etc., a set of data which humans did not interfere with is almost unthinkable. In fact, as a very recent report from Deloitte holds, machines can generate personal data, for example through geolocalization systems. In the same way, people can generate non-personal data, whenever they contribute to a semi-automated process of data collection[103].

2.1.2.1 Non-personal and personal data

The latest definition of personal data is the one of the General Data Protection Regulation, according to which "personal data means any information relating to an identified or identifiable natural person ('data subject')"[104]. The definition of non-personal data can be extracted from GDPR too and it identifies all data that are not personal. However, this distinction became obsolete[105]. This can be mainly explained by the advances in technologies, that now allow individuals to be connected in every moment of their lives, leaving many traces of their activities and interests[106]. Some examples can be the use of social networks, the use of emails, mobility and sensors[107]. When e-mails are sent, a quantity of data structured and unstructured is generated, especially since modern software and servers allow that also heavy and complex files, such as images, videos and digital documents are sent. Social networks are an obvious tool for data production, as individuals can create their digital-self by sharing all types of information about themselves, from name to job position. However, social networks may be trickier than they seem, as also comments, likes and posts give to people and entities more information than expected, that can still contain information on what people think, like and dislike.

---

102 Yusuf, P., 2017 p.17.
103 Deloitte, 2018.
104 European Union, 2016, Art. 4(1).
105 AGCOM, 2018.
106 A very recent report from Accenture shows all types of personal data, including new recent types that were introduced to be up to date with the digital age. See https://www.accenture.com/_acnmedia/PDF-4/Accenture-Guarding-and-Growing-Personal-Data-Value-POV-Low-Res.pdf
107 AGCOM, 2018, p. 32.

Mobility is another way of producing data, as devices that record location and movement are now very widespread. Other than being very pervasive, because it is always possible for operators to know where we are, also our preferences can be tracked through this process. A common example is that the addresses that identify our devices can be recognized by sensors in shops and used to deduct important information, such as how much time a customer spends in there, how he or she moves in the shop, therefore what he or she likes[108]. Finally, sensors in general can produce many data and they seem to be the most pervasive technologies. Other than geolocalisation, sensors can identify and collect even biometric data (for example, more and more devices now have facial recognition) and data about health, such as heartbeat, posture, body temperature, sleep etc. Because of all these developments, the concept of "quantified self" emerged[109]. This term refers to the habit of self-tracking, that consists of collecting and analysing health-related data and using it to improve and in general control one's health condition. This concept will be further analysed in the third chapter.

However, all the examples of personal data that were named above have a common trait, which is fundamental to understand why personal data protection is increasingly a hot topic of these times: because of all these technologies, more and more often the individual is not fully or at all conscious of providing different types of operators with his personal data.

To describe more comprehensively how personal data originate, a new classification was introduced by the OECD, based on different levels of data providers' awareness[110]. According to this criterion data can be provided, observed, derived and inferred.

Provided data are on the highest level of awareness of the individual, who practically takes action to generate them. These are in turn divided into initiated, transactional and posted. Initiated data are created when the individual spontaneously provides data that are needed to begin a path, such as the opening of a mortgage or simply the subscription to a gym or a website. Transactional data, as explained in the previous paragraph, are generated during a transaction. The individual knows that a transaction is usually recorded, especially with the use of credit cards and other cashless payment methods. Posted data are the result of the free expression of the individual. While in earlier times, this type of information was usually found in newspapers or television, with the spread

[108] Ibidem.
[109] Lupton, D., 2013.
[110] Abrams, M., 2014.

of social networks this type of data increased dramatically. Suffice it to say that in one day 200 million tweets are written[111].

Observed data "is simply what is observed and recorded"[112]. They can be further divided into three categories. The first one is engaged data, that are produced in a way in which the individual only realizes the observation at a certain point and can decide to stop it. Once the example for this category was cookies, as before GDPR not all websites were letting the user know about them. The second sub-category is anticipated data, that are originated when the person knows that there are sensors which may be observing him, but is not aware of the fact that the data created may be about him. Finally, passive data are data that are not actively created by the individual. An example is the use of facial recognition in public places for security reasons.

Derived data are new data elements produced in a digital way that pertain to someone just by being derived from other data related to the same individual. They can be split into two types. The first one is made of computational data, in which the new data element is the result of calculation made with other available data. The second is notational data that is the fundament of marketing segmentation, as individuals are inserted in a segment with other individuals based on common attributes.

Finally, there are inferred data, in turn divided into statistical and advanced analytical which refer to data obtained through probabilistic analytical processes. Statistical data are mainly the result of statistical processes and advanced analytical are data obtained through calculations aimed at finding correlation in very big datasets. Both in computational data and in inferred data the individual is not aware at all of the fact that new data elements that pertain to him are being created. This new classification also gives us better insights on the difference between machine-generated data and human-generated data, that became obsolete too as anticipated in the previous paragraph. In fact, most data still somehow rely on the interference of individuals.

In conclusion, it is possible to notice that very often in the literature, scholars write about data in general, without distinguishing between personal and non-personal data. Most of the attention however, is usually dedicated to personal data, to the risks deriving from their usage in business contexts and to the development and implementation of tools for protecting them. Also, the focus of the rest of this dissertation will be mainly on personal

---

111 Retrieved from https://www.forbes.com/sites/kalevleetaru/2019/04/23/a-fading-twitter-changes-its-user-metrics-once-again/#587865ff7a31 .

112 Abrams, M., 2014, p.6.

data. Nevertheless, it is worth mentioning that very recent developments in the data regulation framework at a European level pertain to the free flow and protection of non-personal data, as their societal and economic benefits become more clear day by day[113].

2.1.3 Personal data in the Smart Factory: benefits and misuse.

As briefly introduced at the end of chapter one, data protection is one of the challenges of the Smart Factory, as in this environment the interaction of Cyber-Physical Systems in the Internet of Things allows the generation of big quantities of data. Identifying personal data in this environment is necessary to understand how current protection tools are being employed or should be improved. Three main areas in which personal data benefit businesses can be identified: customer innovation, product innovation and market innovation[114].

For what regards customer innovation, the benefits of data analytics are very evident in customer relationship management and the enhancement of customer experience. The use of data is fundamental to give to customers what they really want, as it allows an increasing degree of personalization, a fast assessment of success and thus, almost real-time response, resulting in customer satisfaction and positive economic indicators. A survey carried out by Accenture showed that 53% of respondents believed that data analytics allowed the enhancement of customer loyalty[115]. A good example of customer innovation is reported in a McKinsey study, that reports that a potato-chip manufacturer wanted to improve the taste of their products in a very accurate and detailed way, carefully measuring the spiciness level in particular. To reach this aim they implemented different types of customer data analysis. From basic ones, such as asking a panel to rate the spiciness of different potatoes on a scale from zero to ten, to developing sensors that could actually taste spiciness. "Within a year of implementing the program, customer complaints about variability in the flavor of the company's chips dropped from 7,000 a year to fewer than 150—a decrease of 90 percent."[116]

---

113 Free flow of non-personal data is acquiring increasing attention from the European Union, which considers it one of the objectives that have to be pursued to implement the Digital Single Market. Just in June 2019, a new regulation disciplining this issues was enforced. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN

114 Cooper, T., LaSalle, R., 2016.

115 Ibidem, p. 9.

116 Fritzen, S., Lefort, F., Lovera-Perez, O., Sänger, F., 2016, p. 2

Finally, personal data can also unlock the potential for product innovation. This can happen in many phases of the development process, such as the generation of ideas one, the design and engineering one and the test and launch one[117]. In the first case consumers, especially those who are labelled as lead users, become the source of new concepts or the means to assess others' ideas. One example is Oreo, that for some years now has been promoting the "#MyOreo Creation Contest", that invites people to propose a new taste for the filling of the famous cookie[118]. However, customers can be included in a deeper way, when they are called to take action and be part of the design process. Even luxury brands, such as GUCCI, now give the possibility through virtual dialogue pages to actually design certain features of their products. In this case, customers not only give an indication on tastes and preferences anymore, but actually become creative designers. Finally, in the test and launch step, the customer can not only give feedback but also directly improve the product. For example, Testbird is a new online service that allows you to enter a network of testers and be paid to fix bugs in your spare time[119].

Although data can benefit businesses in many ways, many risks can arise from a bad management of this asset. At the end of chapter one information security was identified as one of the main challenges of the Smart Factory, but the risks outlined were mainly related to non-personal data. These factors are very important especially because they are related to the correct conduct of the production process and to environmental and employees' safety, however risks can arise also from the presence of personal data in the factory. Defining and explaining these risks is not an easy task as very often the damage cannot be predicted or quantified easily. A good path to start is dividing them between those pertaining to the data holder and those about the data subject.

The main risk that could damage a company is a data breach, that was defined as "'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."[120] This type of events is getting more and more attention due to their increasing frequency, impact and quantity of compromised data. From these statistics, it is possible to observe that data breaches can be not only the result of actions carried out with malicious intentions, but also of the loss of a device containing this information, or accidental

117 Zhan, Y., Tan, K., Hua, L., Yina, T., Ying K., 2018.
118 #MyOreo Creation Contest at https://mondelez.promo.eprize.com/myoreocreation/ .
119 Testbird main page https://nest.testbirds.com/home/tester .
120 European Union, 2016, Art. 4(12).

sharing by employees. Data breaches can be classified according to many criteria, such as the area of occurrence (most of data breaches usually take place in North America) and what technology was used[121]. A very interesting fact is that data leaks are mainly caused by internal breaches, which implies that also non-technological solutions have to be found[122]. Always under the data holder perspective, the main damage arising is the cost of the breach. Annually IBM and the Ponemon Institute publish their "Cost of Data Breach Report", that provides the reader with insights on the generation of it and how to minimize it[123]. According to the 2018 edition, the average cost of a data breach in the reporting year was 3,86$ million with a rise of 6,4% compared to 2017. Many different elements participate in the formation of this value, to a different degree. In 2018, only 4,1% of the average cost was actually caused by the notification of the breach, that results in different types of interaction with the regulator and usually the payment of a fine. The other factors that contribute to the cost are the expenses arising from the post-breach response (26,4%) and from the detection and escalation of the breach (31,8%) and finally, the biggest share belongs to the lost business costs that make up for 1,45$ million. In details, this cost consists of the sudden loss of customers and the increasing difficulty of customer acquisition and the diminished reputation and goodwill. The lost business factor, as the share in the total average cost shows, is a very important factor. However, as Acquisti points out, customers can "punish" companies that they do not consider trustworthy not only after something happens, but also ex-ante, when they are afraid that they will have privacy problems in the future[124]. According to many recent reports, the trust of consumers in companies is in fact fading and they are often perceived as the main responsible entity (together with governments) for privacy risks[125]. Finally, one last indicator that estimates the loss of businesses due to privacy concerns is the stock market value. According to a study conducted in 2018, in the long run, firms that suffered from data beaches tend to underperform the market[126].

---

121 Retrieved from https://breachlevelindex.com/data-breach-library .
122 Cheng, L., Liu, F.,Yao, D.D., 2017.
123 Ponemon Institute, 2018.
124 Acquisti, A.,2010, p. 21.
125 See for example https://www.pwc.ru/en/retail-consumer/publications/assets/pwc-global-state-of-information-security-survey-retail-and-consumer.pdf or https://www.akamai.com/us/en/multimedia/documents/report/akamai-research-consumer-attitudes-toward-data-privacy.pdf
126 Comparitech, 2018, retrieved from https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/ .

Regarding the damage for the data subject, different types of data risks can occurr, but they can be divided into two main categories, i.e. repurposing and data breaches. Repurposing refers to "the use of data for a purpose different from that for which it was originally collected"[127]. Profiling is a very tricky aspect of repurposing, as very often it is actually declared, yet the customer does not fully understand what it may result in. This privacy risk draws a lot of attention in the environment of Smart Factories as very often it is caused by automated decision-making and by the abilities of machines to infer new data elements from large datasets. The relationship between consumers and this practice is nevertheless controversial, because although very often it is perceived as creepy, consumers seem to be still very willing to share data in exchange for benefits[128]. However, profiling can in fact be very intrusive. One obvious result of profiling is price discrimination, which takes place more and more often. For example, Home Depot's online prices are based on the distance between the customer searching the page and the store, while airlines prices change according to many criteria, from the fare to the time of the day[129]. Profiling can get worse, when it is based on sensitive data, that are data pertaining to more sensitive characteristics of the subject, such as his ethnic origin, health and sexual life, or his opinions regarding religion and politics. Profiling according to these data may even lead to discrimination. For example, in the US it was reported that some stores were lowering credit limits as a consequence of negative repayment statistics of other people shopping at the same stores[130]. Another consequence of repurposing is the sale of data to a third party. As it was observed before, this can benefit businesses as data in this case acquire a real monetary value. Conversely, for the data subject this can result in further data misuse from the third party.

Like for data holders, some risks for the data subject can arise from data breaches. The consequences of such events are very difficult to describe and quantify. In some cases, the entity that acquires the data (both in a malicious and in a casual way) will use them or misuse them in the same way and for the same purposes as the previous holder. In other cases, the worst, data breach can lead to identity theft, which refers to when an individual's personal information is stolen and then used in an illegal way.

---

127 Information Commissioner's Office, 2017, p. 11

128 Retrieved from https://dma.org.uk/uploads/misc/5b2a5cd7c0268-consumer-privacy--01_5b2a5cd7c01d1.png .

129 Retrieved from https://www.forbes.com/sites/neilhowe/2017/11/17/a-special-price-just-for-you/#2bffa1c390b3

130 Information Commissioner's Office, 2017, p. 20.

2.1.4 Protection tools

As the concerns for privacy risks keep growing, so does the number of tools available to firms in order to protect themselves and their customers. Some important instruments are de-identification techniques, privacy notices and privacy-by-design[131].

De-identification techniques are mainly anonymization, pseudonymization and encryption[132]. Anonymized data refer to data that allow the identification of a person neither individually nor in combination with other data. The insights of anonymized data are still very useful in helping companies to develop products and services and they mitigate the risk associated with the loss or malicious breach of datasets. However, there is no way to assess that data have been perfectly depersonificated, or that it is impossible to reconduct, with the use of other data, the anonymised data to the individual they pertain to. Anonymization has shortcomings too, as it cannot be reversed. In the field of healthcare, this technique is very common as health information is not only personal but also very sensitive. Nevertheless, after a data element has been anonymised, the patient cannot be contacted anymore when further information or treatment is required[133]. An alternative to this technique is encryption, that refers to when the data elements are converted to another form and only some chosen individuals have the so-called decryption key, that can convert the encrypted data to its past form. However, this presents disadvantages too, as this kind of data protection implies the loss of meaning of the data in the case of re-use, unless the owners of the key reverse the process, thus becoming identifiable again. The last de-identification technique is pseudonymization, that seems to unite the strengths of the other two techniques[134]. In fact, the protected data elements pertain to pseudonyms, that cannot be linked to the data subject without knowing the secret key. In this way, the process is still reversible, but the data are retained in an anonymous form.

Another tool commonly used to protect customers is privacy notices. This tool has a great theoretical value as it is specifically aimed at ensuring transparency. Big data are intrinsically opaque, due to their association with artificial intelligence, automated-

131 Information Commissioner's Office, 2017
132 Ibidem, pp. 73-74.
133 Heurix, J., Neubauer, T., 2011.
134 Ibidem.

decision making and machine-learning. The fact that almost every aspect related to data collection, storage and analysis depends on advanced algorithms makes it very difficult to understand, almost ineffable. Opacity can arise from different sources. The first one is the need for corporations to actually protect their algorithms, as they can be the source of competitive advantage. The second is that typically algorithms and coding are not subjects known by many people, therefore this type of opacity could be fixed by increasing education and making this knowledge more accessible. Yet, the third source of opacity is related to the actual difficulty of algorithms, not only because they are usually the result of the interplay between many engineers and sometimes being able to read codes is not enough, as the way they operate with data could still be not manifest[135]. Because of all these reasons, companies have to be committed to transparency in a way that customers can trust the company regardless of the opacity of the subject. The privacy notice is a transparency requirement and as such, it should provide very detailed information, from the exact purposes the data will be used for to how the automated decision-making process happens and everything should be expressed in clear terms for customers. Although concerns for privacy and transparency are on the rise, still very often customers do not read privacy notes and this should stimulate companies to find a creative and innovative way to inform their customers in an accurate way[136].

Finally, Privacy by Design is the most innovative and comprehensive tool for data protection, as it aims to ensure the pursuit of privacy protection through every phase in the development of a service or a product. This concept, which was theorised by Ann Cavoukian in Canada in the late 1990s, came to be known and accepted internationally at the 2010 Assembly of Privacy Commissioners and Data Protection Authorities a resolution involving this concept was passed. Privacy by Design as described by its founder relies on seven main principles[137]. First of all, protection should be preventive, that is aimed at avoiding privacy intrusions before they happen. Then privacy should be the default rule, meaning that individuals do not have to worry about protecting their data as privacy should be already the standard. This is related to principle three, that is the embeddedness of Privacy by Design in the architecture of businesses and IT processes. However, this should not hinder the functionality of businesses practices, nor generate trade-offs of any kind. This results in principle four, which holds that Privacy by Design

135 Burrell, J., 2016, pp. 3-4.
136 Information Commissioner's Office, 2017, pp.61-63.
137 Cavoukian, A., 2010.

should generate a positive-sum, a win-win situation for all the entities involved. The fifth pillar is that the concept should not only be embedded in every part of the business architecture, but also in the whole life of the data that have to be protected, from collection to use, generating end-to-end security. Finally, Privacy by Design has to be open and user-centric. The feature of openness refers to the fact that the concept has to deliver the results that it promises while being transparent and subject to independent verification. Thus, all these features together aim at ensuring the privacy of customers, therefore user-friendliness, i.e. putting the user's interests above all, is the seventh fundamental principle[138].

Although very often this tool is considered the ultimate solution for data protection and much attention has been given to it (it was also included in the GDPR), still the concept per se attracted some critiques too. The main observation that was opposed to Privacy by Design is that it is too vague[139]. In fact, rather than a concept it seems to be a suggested approach that nevertheless does not refer specifically to any device, system or industry and does not provide any formal rule or standard[140]. Furthermore, a fundamental aspect of Privacy by Design is that it should find the perfect balance between Privacy Enhancing Technologies (PETs) and Privacy Invasive Technologies (PITs) that, as mentioned before, only generates a win-win situation. Although Privacy by Design puts a lot of emphasis on this technological aspect, it still seems to be too focused on data protection, neglecting all the risks generated by modern PITs[141]. However, this could also be seen as a matter of interpretation of the dichotomy Privacy and Data Privacy, which will be analysed in the next paragraph.

As mentioned before, de-personification techniques, privacy notices and Privacy by Design are some of the tools that companies can use to guarantee that they are maximizing data protection. However, the problems arising from the fact that people create and access an enormous quantity of data every minute cannot be limited to some risks that may undermine the relationship between people and businesses. The consequences of such data-driven environment are way more complex and can entail even a decrease of welfare, which is why the importance of Privacy Law grew hand in hand with Big Data. However, this process was uneasy too. In fact, by now there is still lack of agreement among

138 Ibidem.
139 Klitou, D., 2014.
140 Klitou, D., 2014.
141 Ibidem.

scholars on whether data regulation actually benefits the public interest and, if it does, what the rights amount of it is. Regardless of this debate, it is undeniable that Europe in particular has adopted a regulatory approach towards the issue of data protection, which was also recently revolutionized with the enforcement of the General Data Protection Regulation. In order to gain a comprehensive understanding of how to adjust the protection of data to a concept that is mainly European and that propelled even more the importance of information in a business environment, it is vital to analyse the history and development of data regulation. This will be the assignment of the next paragraph.

2.2 A History of Data Regulation

2.2.1 Is data regulation necessary? A matter of trade-offs.

As anticipated in the previous paragraph, there is no agreement on the actual necessity of data protection. As Acquisti reports, some scholars, mainly associated with the Chicago School, believe that regulating privacy actually results in diminished welfare[142]. Some of their theories are based on the belief that there is a trade-off between data protection and the amount of information available to pursue innovation and other social goals, i.e. a trade-off between privacy and efficiency[143]. This mainly happens when data protection is equated with concealment[144], as according to this interpretation, data are being withdrawn from other operators that could use it in an efficient manner. Probably, this resembles what customers think when they give some of their data, expecting tailored offers and contents from the service providers. Another famous theory is the one of Stigler, who believes that regulation would generate a redistributive effect and inefficiency, by removing the possibility to assess the quality of information available[145]. In fact, people normally share data when they have positive facts or characteristics to show, while those who have something to hide do not disclose personal data, practically admitting that. Finally, also the Coase Theorem has been used to prove that data protection generates inefficiencies, as according to it, in presence of externalities, private operators can negotiate and internalize them, eventually reaching a better equilibrium of resources[146].

142 Acquisti, A., 2010, p. 5.
143 Cofone, I., 2017, p. 521.
144 Acquisti, A., 2010.
145 Stigler, G., 1980.
146 Coase, R.H., 1960.

A recent piece of research by Cofone sums up the critiques that were opposed to these theories[147]. According to him, the idea that there could be a trade-off between efficiency and availability of information is originated by an instrumental interpretation of the concept of privacy, i.e. that it is only used to hide something and then get something else in return. However, privacy can have an absolute value and people can have pure privacy preferences. If this is true, then it cannot be taken for granted that the utility arising from getting the information regarding some individual is bigger than his disutility in losing it. Another aspect reported by Cofone is that the Chicago School analyses privacy in a way that only includes static effects. When considering dynamic indicators too, privacy may end up incentivizing the creation of information. One example is that with a total lack of protection, many people who value privacy per se could decide not to join social networks or any kind of service or activity that entails the disclosure of data, that, as a consequence, would not be created at all. Providing some level of protection, instead, would result in "a high level of information production (dynamic effect) but a low level of information flow (static effect)"[148]. Finally, the government has to find the level of privacy that maximizes the production of data, without decreasing the flow of information. The representation of this level is the peak of a hill-shaped function (Figure 7).

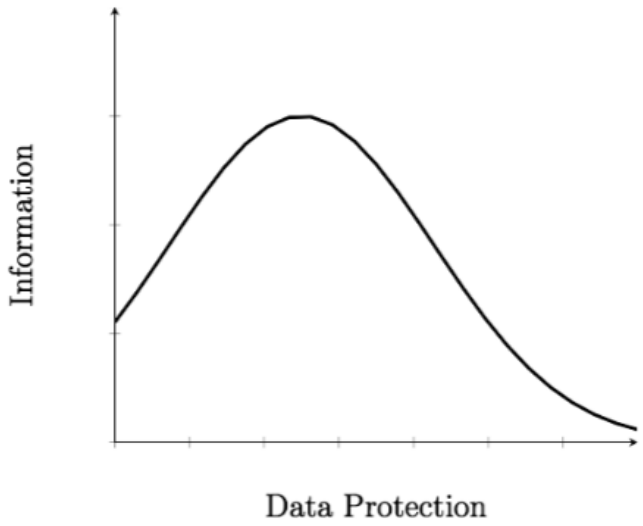

Figure 7 - Relationship between Information and Data Protection (Cofone, I., 2017 p. 541)

147 Cofone, I., 2017.
148 Ibidem, p. 540.

Previously, the most practical aspects of usages and risks deriving from personal data were illustrated, together with some technological tools that corporations can use to guarantee a certain degree of protection. This paragraph, instead, showed that the relationship between data availability and data protection is much more complex: through economic theory, it was demonstrated that a wrong level of protection may even affect welfare in a negatively, thus requiring the intervention of the government. However, the motivation and path that lead Europe to become the "leading paradigm in information privacy"[149] go beyond both practical aspects and economic theory, as it is founded on the belief that privacy is a fundamental human right and that it must be protected at all costs.

2.2.2 Privacy as a right: the basis for data protection

The modern concept of privacy originated in the United States and traces back to the end of the 19th century, when two lawyers, Samuel Warren and Louis Brandeis published a paper called "The right to privacy". In that paper they first theorized this concept, defining it as "the right to be let alone"[150]. The publication of the article was probably stimulated by increasing media intrusion, in turn propelled by the invention, some years earlier, of the mobile camera by Kodak[151]. The authors believed that men were turning more and more to privacy and solitude as an escape from the increasing complexity of the world, but new technologies that intrude privacy started spreading, causing psychological pain and distress. As a consequence, law had to evolve and defend the expression of intangible spheres of men's lives towards his productions, publications and compositions (that were already protected by copyright law).

This right gained international recognition right away, as in 1950 it was introduced in Article 8 of the European Charter of Fundamental Rights:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public

149 Ibidem, p. 521.
150 Warren, S.D., Brandeis L.D., 1890.
151 Wacks, R., 2010.

safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[152]

As it is possible to observe from Article 8, in the European framework the right to privacy is very broad and covers also other rights, such as respect for family life and correspondence, protected in turn by other areas of EU law[153]. While according to some scholars privacy is a value itself, according to others it relies on other values, such as dignity and autonomy, as the possibility for individuals to shape and be in control of their own lives[154]. Another aspect of the concept of privacy that is largely debated is its scope. The right to privacy as stated in Article 8 seems to mainly pertain to private life, which in turn refers to everything that is not public. Nevertheless, with the advent of the internet and of the information society, the boundaries between the public and private sphere of the individual becomes blurred, leaving a lot of room for different interpretations of the scope of privacy. One very common debate related to this topic is the one on the relationship between privacy and data protection.

2.2.2.1 An open debate

As Gerards points out, privacy is one of the "first generation rights" that, as such, has a negative trait, i.e. the government has to protect the individual from possible interference against the exercise of the right[155]. The first level of protection pertains to civil and political protection and, in the case of Article 8, ensures that the state does not intrude the private life of the citizen. Second generations rights instead, or peripheral rights, concern the social and economic spheres. The European Convention of Human Rights was designed as an instrument to create only first generation, negative rights. However, observing the case law history of the Convention, it is possible to see that the line between negative and positive rights became blurred very soon. The first famous case concerning Article 8 was the Lòpez Ostra one[156]. The Lòpez family came before the court because a plant for the treatment of solid and fluid waste near their house was causing health problems to the members of the family, by polluting the whole neighbourhood. Although this may seem a case for environmental law, in the final verdict, not only the right to

152 ECHR, Article 8.
153 Hijmans, H., 2016.
154 Ibidem, p. 41.
155 Gerards, J.H., 2008, pp. 656, 657.
156 ECtHR, 1994.

health was considered, but also the right to enjoy your home, that was hindered by severe pollution[157]. This demonstrated that also individual interests could be protected through the instrument of the European Convention and in the following years the doctrine of positive obligations expanded further, so that many other economic or social interests were brought under the umbrella of the Convention by the Court. As a consequence, the concept of privacy became very broad and dynamic and interference with this right started to be evaluated according to the context[158]. With the development of the internet, the scope of the right to privacy had to be reinterpreted again. Put simply, privacy on the internet naturally refers to informational privacy, as there is no physical or spatial dimension (such as the home) and interferences with this right that are associated to data protection became very frequent[159]. When relying on the approach of contextual evaluation, one could try to assess whether interests related to data protection can be brought under the scope of the right to privacy, that is what Hijmans did[160]. The author identified four types of interests that concern data protection, but still have an impact on the right to privacy: the processing of information by governments for law enforcement, the processing of health-related information, the protection of vulnerable groups and the reputation of people in publications. By analysing some significant cases, Hijmans demonstrated that all these interests fall under the scope of the right to privacy, however the debate still remains unsolved:

> "this does not answer the fundamental question of whether all use of personal information – or, in the terminology of data protection law, all processing of personal data – falls within the scope of the right to privacy and creates interference with this right. This question can also be formulated differently: are qualified interests a condition for bringing the use of personal information within the scope of the right to privacy, or are they merely relevant for assessing an interference with this right?"[161]

A similar, yet different approach is the one of Herth and Gutwirth[162]. These authors, like Gerards, recognize the negative trait of the right to privacy. Data processing, instead, is not just prohibited in general, thus data protection is positive by nature and acts as a catalyst of power in order "to promote meaningful public accountability, and provide data subjects with an opportunity to contest inaccurate or abusive record holding practices."[163]

---

157 Gerards, J.H., 2008, p. 660.
158 Hijmans, H., 2016, p. 47.
159 Ibidem, p. 40.
160 Ibidem, pp. 44-46
161 Hijmans, H., 2016, p. 47
162 De Hert, P., Gutwirth, S., 2006.
163 Ibidem, p.16.

In this sense, the right to privacy is an opacity tool, while the right to data protection is a transparency tool. Finally, these two rights should not exclude each other as their two aims (limiting power and catalysing power) are actually each other's supplement. Another significant point is finally added, concerning the fact that privacy is a value per se, while data protection is not, as it is rather a set of procedures that should be used to protect specific interests[164].

The theoretical debate on whether the concept of privacy and data protection overlap is still unsolved. However, as Hijmans illustrates, what matters in the end is that at a European level also the right to data protection developed, as we will see in the next paragraph, and by now both rights exist as fundamental rights that are part of one system[165]. Privacy is broader and, moreover, it represents a value linked to human dignity and autonomy. Data protection instead is one of the means of guaranteeing privacy, especially in a time when all aspects of data protection have the power to affect people's privacy.

2.2.3 OECD Guidelines

Before appearing into European regulation, the data protection concerns were acknowledged by the OECD in 1980 in the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"[166]. Although the principles stated in the document were non-binding, their importance is still widely recognized, mainly for the great influence they had on the creation of European and national legislations in the following years. It is also necessary to introduce the topic of data protection with the OECD guidelines because this entity is still very active in this field, although normally it should not be involved in issues regarding the protection of fundamental rights, as its scope mainly pertains to technological and economic issues[167]. However, when the expert committee reunited not only had privacy become a fundamental human right, but many writings on that value started encompassing concerns about data protection, especially caused by the rise of automated data processing. As a consequence, the OECD took the challenge and the opportunity and understood that only an "intercontinental solution"

164 Hijmans, H., 2016, p. 68.
165 Data Protection was introduced in Article 8 of the Charter as a separate right from that of privacy.
166 OECD, 1980.
167 Kirby, H., 2012.

could address the cross-national trait of data flow[168]. The reason behind this choice was closely related to the presence of the United States amongst the members of the OECD. In fact, as Kirby points out, by the time the expert committee started meeting it was already clear that the United States had a prevalent position for what regards data processing and it was known that a binding treaty with Europe would have sounded suspicious. At the same time, on the European side, there was the fear that the response to trans-border data flow privacy concerns would have been the erection of economic barriers[169]. Thus, the real trigger for the intervention of the OECD, an entity mainly concerned on economic and technological issues, was the matter of barriers.

The main result of the expert committee was the identification of eight fundamental principles that still today influence the discourse on privacy and data protection[170]:

- Collection limitation: This principle entails that data collection should be limited as possible and that, when personal or non-personal data are obtained, it happens by lawful and fair means, with the awareness and approval of the data subject.
- Data quality: This principle refers to the relevance of personal data for the purpose for which they are obtained and, relative to that purpose, to accuracy, completeness and up-to-dateness of the data.
- Purpose specification: This principle states that the data subject should be made aware of the purpose for which personal data are collected not later than the moment of the collection and that then the use of data should be limited to the fulfilment of the purpose. Every change in the subject should be specified too.
- Use limitation: Personal data should not be disclosed, made available or used for purposes other than those specified as according to the previous principle, unless required by the law or with the approval of the data subject.
- Security safeguards: There must be security safeguards that protect data against loss, unauthorised use, destruction, use, modification and disclosure.
- Openness: This principle refers to the fact that it should always be possible to know what the nature and use of personal data as well as who the data controller is and his usual residence. In general, all developments, practices and policies relative to personal data have to be kept open.

168 Kirby, H., 2012, p. 7.
169 Ibidem, p. 8.
170 OECD, 1980.

- Individual participation: This principle lists all the ways in which an individual can be responsible for his own data. He has to be able to have confirmation from a data controller that the data controller has data relating to him. Then, data relative to an individual should be communicated to him in a timely manner, at an inexpensive charge, in a reasonable way and in an intelligible form. Moreover, the individual should be able to take action in case the previous rights are denied to him and finally, if the challenge is successful, data should be erased, updated or corrected.
- Accountability: The data controller has to comply with measures that ensure the previous rights and held accountable for compliance.

As mentioned before, these guidelines were the first impressive step towards data regulation. The innovative reach of this document can be explained by some main aspects. First of all, they are technologically neutral, i.e. they are not limited to automated data or to any industry, as well as to no sector, whether private or public[171]. Secondly, they are written in a language that makes them both non-binding, as it appears from the use of the verb should and of structures non-typical of treaties, and very easy to understand, with a simplicity that ended up being perfect for the kind of complex evolution of the subject. Moreover, the guidelines add the principle of accountability, which had never appeared in earlier works. Finally, the most important point is that the eight principles call Member States to action but leaving space for flexibility. They gave a direction, allowing at the same time Europe to proceed on its path towards data protection and other countries to have a softer approach, without neglecting the underlying issue. As Kirby points out "they thereby imposed duties of imperfect obligation. But they were duties nonetheless. And, on the whole, have been taken seriously by the countries that are parties to the OECD Convention."[172]

For all these positive characteristics, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were used for more than 30 years without any change and successfully paved the way for a comprehensive legislative framework, especially in Europe as only one year later the Convention 108 on Data Protection was passed and became the real landmark of European data regulation. However, before proceeding to the analysis of the latter, it is worth mentioning that although the guidelines served their purpose for more than thirty years, they also kept evolving, thus being subject

171 Kirby, H., 2012, pp. 10-11.
172 Ibidem, p. 11.

to a general revision in 2013. Of course, from 1980 much changed for what regards data processing: the World Wide Web and Google emerged, social networks were invented and started to spread, thus risks arising from data grew in number and complexity. This stimulated the revision of 2013, which mainly entailed a switch of focus from the individual from data collectors and data users, strengthening the principle of accountability, according to which now data holders have to not only comply to measures that guarantee a safe data environment but they also have to demonstrate to regulators that they are able to comply. The 2013 revision also distinguishes data collection from data use more clearly, with different principles pertaining to each phase, always to shift responsibility away from individuals[173].

2.2.4 Convention 108 on Data Protection

The Council of Europe Convention 108 (Convention for the protection of individuals with regard to automatic processing of personal data) of 1981 is the first binding instrument that focuses exclusively on data protection, which is described as to respect the individuals' "rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him"[174].

The first fundamental aspect of this document is its value as a binding instrument. However, from the content point of view, Convention 108 is half-way between the OECD Guidelines and the European Directive 95/46. Many aspects are specified in a more clear and concise way by the OECD Guidelines, while the Directive, despite being interpreted not only as a specification of Convention 108, it is the actual main source for data protection as a fundamental right.

A good methodology to understand the differences between these documents was proposed by Greenleaf, who considered a distinction between global and European elements[175]. The former refers to those elements that are shared between the OECD Guidelines, the APEC Privacy Framework[176], the European Directive 95/46 and the Convention 108. Some of them directly identify some of the principles of OECD, for

[173] Ibidem.
[174] Council of Europe, 1981, Art. 1.
[175] Greenleaf, G., 2012.
[176] APEC stands for Asia Pacific Economic Cooperation and refers to a regional economic forum that promotes growth through economic integration. It was established in 1989 and it has 21 members. The privacy framework aims at integrating privacy protection across the members without obstacling information flow. It was endorsed in 2005. Available at https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

example Collection Limitation, Data Quality, Purpose Specification, Openness and Accountability. Others instead appear in all the instruments but in a different way compared to the OECD, such as the right to Notice at the moment of data collection, which is ambiguous in the OECD Guidelines and the right to correction and access, that are just a part of the Individual Participation right[177]. These global elements are somehow the core of data protection law, as somehow they are always found. The latter (European elements) are those that are only present in the Directive 95/46 and in Convention 108. These regard collection, that does not only have to be limited but it also has to be the minimum necessary for the purpose of collection; fairness and lawfulness, that do not have to be applied only during collection but also through processing; erasure or de-identification of personal data after a certain period; further protection for special categories of data[178]. Finally, there are some elements that Greenleaf defines always as European but they are shared between the Directive 95/46 and the Protocol of Convention 108. The 2001 Additional Protocol (ETS 181) aimed at filling some shortcomings of the Convention, thus it added dispositions on the flow of personal data to other countries, an independent supervisor authority and the right to challenge issues relative to data protection before a court. However, with such amendments Convention 108 was brought to the same level of Directive 95/46[179].

So, if the principles of Convention 108 could be found both in the OECD Guidelines and in the following European Directive, the real innovative reach of this document was to be found in some other aspects. However, the fact that the Convention is the first binding set of rules on data protection is sufficient to assess its importance. Although now the Directive is on the same level, the latter would not exist without the impulse given by Convention 108. Also, the distinction made by Greenleaf between European and global elements is aimed at identifying how many non-European legislative frameworks of data protection were influenced by the Convention (plus its additional Protocol) and the Directive 95/46 and the results are striking[180].

Finally, the real innovative reach of Convention 108 can be found in the possibility given to non-European countries, already from 1981, to accede the Convention and, since 2001, its additional Protocol too. In particular, the Convention 108 is the first instrument that

177 Greenleaf, G., 2012.
178 Ibidem.
179 Greenleaf, G., 2012.
180 Ibidem.

officially states the unilateral regulatory power of Europe in the field of data protection too[181]. In a famous article called "The Brussels Effect", Bradford observes that while many flaws of Europe are globally manifest, such as the weak military power and the inability to speak with one voice, an ability that is often neglected is that Europe is able to regulate global markets unilaterally[182]. Thus "the European Union sets the global rules across a range of areas, such as food, chemicals, competition, and the protection of privacy"[183]. In conclusion, the same happened with data protection, as the European Economic Community could use the Council of Europe and the Convention 108 as facilities to export the data protection European regulatory system, thanks to the possibility of accession[184].

2.2.5 European Data Protection Directive

The Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data constitutes the first appearance of the right to data protection in European secondary law. This new set of rules, promulgated in 1995, was fuelled by the increased use of data in many industries and fields, consequent to the spread of Information Communication Technologies in the 1970s. The content of the Directive is not particularly innovative, as it follows closely that of the OECD Guidelines. However, there are two main aspects that are relevant: first of all, the protection granted by the principles addresses the freedom of individuals and their privacy, especially relative to data processing. Secondly, it promotes the free flow of information in the internal market of data[185]. By the time the Directive was promulgated, the European data protection framework was far from being harmonised: some countries took action, by imposing limitations and procedures, while others were still completely unregulated[186]. As a consequence, the Directive was conceived as a tool that, by harmonising the data protection practices in Europe, could promote the existence of an internal market of data too.

---

181 Bradford, A., 2012.
182 Ibidem.
183 Ibidem, p. 3.
184 Hijmans, 2016, p. 487.
185 Ibidem, p. 50.
186 Robinson, N., Graux, H., Botterman, M., Valeri, L., 2009.

The central point of the Directive 95/46 is data processing, including further processing of data that were collected for a different purpose. According to the interpretation of Elgesem, this constitutes a switch of focus, that in earlier legislation was on data collection[187]. Acknowledging this is very important, because it shows that the European regulatory framework evolved in accordance with the needs of the market and individuals. Only by guaranteeing the respect of privacy in the various phases during the processing of personal data, the harmonisation that Europe needed could be reached. Furthermore, the Directive acknowledges that most of the information used nowadays is the result of the analysis of other information, that was already produced. Thus, it addresses also the processing of data that were collected for a different purpose[188].
The result, as Robinson et al. point out, is that "comparable legal rules for crucial aspects of personal data processing are in place throughout the EU. These include the concept of personal data, requirements for legitimacy, data quality and security, data subjects' rights and the possibility of enforcing these rules".

2.2.6 Article 16 of the TFEU

As the Directive 95/46 represented the main appearance of data protection in secondary law, it is necessary to mention how data protection is included in European primary law, that has its source in the Treaties of the European Union. In these documents, not only privacy but also data protection is recognized as a fundamental right, that relies on values that need to be protected in a democratic environment under the rule of law[189]. In particular, Article 16 of the Treaty on the Functioning of European Union is the legal basis of the European data protection framework. The Article lays down the mandate of the European Union for what regards the right to privacy and data protection and disciplines the relationship between European Union and its Member States. Such mandate acts on a constitutional level and the European Union plays the role of a "constitutional guardian"[190].
First of all, it is possible to identify three tasks that the European Union has to accomplish to grant data protection. To begin with, the European Court of Justice has to guarantee

187 Elgesem, D., 1999.
188 Ibidem.
189 Hijmans, H., 2016, p. 71.
190 Ibidem, p. 4.

the respect of Article 8 of the European Charter of Human Rights. In fact, although the first degree of protection pertains to the Member States, as most of the processing happens in or across national jurisdictions, "EU law determines the result – the guarantee that everyone's right is effectively protected – and the Court of Justice of the European Union is the institution ultimately supervising the acts of the Member States"[191].

Secondly, the European Parliament and the Council have to implement data protection legislations. This means that these two entities should establish the rules of data protection, which legitimises instruments such as the GDPR, that can be interpreted as the fulfilment of European Union's mandate.

Thirdly, independent authorities have to be vested by the Union with the power to enforce and control the respect of data protection rules.[192]

From what was observed from the previous lines, it is clear how the European Union became the guardian of the right to data protection. However, the Member States have a fundamental role in all the afore-mentioned tasks[193]. As a matter of fact, responsibility for data protection is a shared competence, meaning that both EU and Member States can promulgate legislative acts. Nevertheless, Member States can only take action to add principles that are not in conflict to those established by the European Union, while on issues that are uncovered, they can fully exercise their competence.

2.2.7 The General Data Protection Regulation

The need for the General Data Protection Regulation can be explained by the shortcomings that the Directive 95/46 started to show at the beginning of the 21st century. The latter, other than focusing on the further processing of data, also aimed at making the flow of data in the internal market smoother and better. However, this change was two-fold. On the one hand, the Directive is still recognized today as the document that first tried to gain policy convergence through a policy instrument. In fact, although there is room for discussion on many points, as showed in previous paragraphs, it "begins a process of codifying a consensus on the most effective ways to implement data-protection law"[194]. As a consequence, by 1996 only Italy and Greece were yet to pass a data protection law. As for outside Europe, the Directive had a big impact too, as in Article 25

191 Hijmans, 2016, p. 133.
192 Ibidem.
193 Ibidem, p. 126.
194 Bennett, C.J., 1997, p. 99.

the transfer of data to a third country is disciplined, stating that it is only allowed when the country ensures and adequate level of protection. On the other hand, as the years went by, the adequacy regime did not yield the expected benefits and interpretation divergences of the principles across Europe started affecting businesses negatively, thus a reform was asked[195].

The first draft of the GDPR appeared in 2012 and was subject to many amendments in the next two years. The final proposal was made by the Council in 2015 and the agreement with the European Parliament was reached in 2016. The General Data Protection Regulation was finally enforced in May 2018.

Much will be written on the innovative reach of this document in the next paragraph, therefore this section will focus on the main advancements relative to the Directive 95/46. The first main changes concern the object and the scope of the protection. Personal data are redefined in a very broad way, so that also information that identifies a person indirectly is included in the set. This is especially important in a time in which IP addresses and cookies are continuously collected without users being aware of the consequences[196]. The scope of data protection is widened too. Similarly to the Directive, the focus is on processing, but that is intended as any activity that can be done with personal data, by organizations or entities that may be located anywhere in the world. As Hoofnagle, Borgesius and Sloot point out, by introducing this advancement, every time a business comes into contact with data that refer to a European citizen, it becomes automatically subject to the GDPR[197].

Some important changes concern the principal actors of data processing and the definition of all their rights and obligations. Already in the Directive, it was possible to find three principal categories, i.e. the data subjects, the data processors and the data controllers. The rights of the data subjects are significantly increased, while new important obligations must be considered by data processors and controllers. First of all, contrary to its predecessor, according to the GDPR processors should be held accountable for any damage caused to personal data too.[198] Another innovative principle is the duty to notify any breach within 72 hours from its discovery. Finally, when the processing of some data

195 Bennett, C.J., 2018.
196 Hoofnagle, C.J., Sloot, B., Borgesius, F.Z., 2019.
197 Hoofnagle, C.J., Sloot, B., Borgesius, F.Z., 2019, p. 73.
198 European Union, 2016, Article 82(4).

is assessed as especially risky for the privacy of the subjects, a Data Impact Assessment must be carried out, to estimate accurately the risk arising from the processing.

For what concerns the rights of data subjects, first of all some important changes were brought to consent, which is the main ground for data processing: in order to be lawful, it must be "freely given, specific, informed and unambiguous"[199]. Moreover, the right to be forgotten has been augmented, as the individual can request that the processors or controllers remove any data that is wrong or irrelevant, according to him. As Tankard points out, this means that "organisations know exactly what information they hold and where it is stored"[200]. In the GDPR also a new right is introduced, i.e. the right to data portability, that establishes that individuals can receive all their data in an intelligible form and move them to a new controller[201].

Other than increasing the rights and obligations of the principal actors within the data protection framework, the approach to the supervisory authorities was completely renewed, towards an increasingly international dimension[202]. These entities "must monitor the application of the GDPR in their respective jurisdictions, and cooperate with one another to effect the consistent application of the regulation across the EU"[203], under the guide of the new European Data Protection Board. Finally, another authority is introduced, the Data Protection Officer, which has to be appointed by the controller and the processor when they carry out processing operations that "require regular and systematic monitoring"[204].

Although all these principles can already convey an idea of how advanced the GDPR is, there are some additional features that pertain to its structure, that give to this instrument a constitutional reach. This characteristic will be analysed in the next chapter.

199 Ibidem, Article 4.
200 Tankard, C., 2016, p. 6.
201 European Union, 2016, Article 20.
202 Bennett, C.J., 2018.
203 Ibidem, p. 242.
204 European Union, 2016, Article 37.

3. Industry 4.0 Bill of Rights: A realistic proposal?

3.1 The Smart Glove: A case study

The assignment of this chapter is to go into the details of the interaction between data protection and the Smart Factory. It was observed that the very fundament of the Smart Factory is the contact between humans and machines, thanks to Cyber-Physical Systems and the Internet of Things. The interaction of these two elements generates a wide amount of data, making their protection one of the main challenges of the Smart Factory. As it was shown, one might think that the importance of information in this context is only related to cyber-security, intellectual property and espionage. This is the result of the wrong assumption that all the data produced only covers supply-chain information and statistics about the production process, exclusively aimed at the optimisation of the factory environment. However, after analysing the increased importance of data, with the objective of finding the reason behind another phenomenon of our times, i.e. Big Data, the assumption was proved to be wrong. In fact, it was demonstrated how, amongst the several categories of data that exist nowadays, the one which poses real problems for protection is the one of personal data, as this type of data is being produced in many and new manners, of which the individual is not always aware. Contrary to what is usually assumed, it was demonstrated that personal data are fundamental in the context of the Smart Factory too, because of the impact that customers have on the supply chain, which they can influence in many ways. All these changes, together with an increased need for harmonisation of European data protection laws, triggered the creation of the General Data Protection Regulation, that has been enforced in May 2018 and is currently the most advanced tool for the protection of individuals concerning the privacy of personal data.
Although some of the limitations of this instrument and its focus on businesses were already shown in the previous paragraph, there is still space for discussion.
A very interesting document was published by the Economic and Scientific Policy Department of the Directorate for Internal Policies of the European Parliament[205]. This piece of research was published in 2016, when the European Parliament and the Council finally agreed on the text of the GDPR, but still sheds light on the possibility of creating a different kind of tool for the protection of data: A Bill of Rights of Industry 4.0.

[205] Gouardéres, F., 2016.

The document observes that in the past years, some companies proposed the creation of an Internet of Things Bill of Rights, to reassert the rights of individuals over their data. The features of such document should rely on the principle of self-determination, which, in the case of information, could be "the most cost-efficient and effective way"[206] to protect data. While the proposals of an Internet of Things Bill of Rights were somehow successful and started a discussion on very innovative concepts like digital constitutionalism, the proposal of the Industry 4.0 Bill of Rights did not appear in other documents following the aforementioned one. Thus, this chapter will evaluate this interesting proposal, by trying to assess whether such a document could be useful. To do so, it will be necessary to understand why such a suggestion was made in the first place, why it was suddenly abandoned and if the enforcement of the General Data Protection Regulation somehow influenced the development of this idea. The starting point will be the same as the Directorate's document, i.e. the smart glove case study. Firstly, this chapter will try to analyse why this specific case triggered the belief that people need to reassess the rights over their data in the authors of the Directorate's document. Then, it will assess whether a Bill of Rights could be the right solution. Finally, it will try to understand how to create an Industry 4.0-specific tool.

3.1.1 ProGlove

ProGlove is a start-up that invented the Smart Glove. It was founded in April 2016, as a response to the 2014 challenge launched by Intel "Make it wearable". The initiative aimed at promoting innovation and creativity in the shape of wearable tools, awarding three teams with over $500.000. Qualifying with a third place, Jonas Girardet, Thomas Kirchner, Alexander Grots and Paul Günther (the ProGlove team) received the $100.000 prize to keep developing their product. In 2016, the München-based firm gathered $2.2 million from Intel Capital, GettyLab and Bayern Kapital, finally being allowed to launch their first-ever industry smart glove: MARK ONE S. The year 2018 was a turning point: ProGlove inc. opened in Chicago and its products were launched in Canada too. After that, the second round of funding began and gathered $6.7 million from Intel, GettyLab, Bayern and a new investor, Deutsche Invest Venture Capital. By the end of 2018, ProGlove was counting more than 130 employees, coming from 40 different countries.

[206] Gouardéres, F., 2016, p. 78.

Moreover, BMW has introduced the smart glove all over its plants in Europe and USA and nearly all European automotive firms use ProGlove by now. As a consequence of this rapid success, at the beginning of 2019, MARK 2 was launched.

Every glove is made of several components. The first one is the wearable glove, that is now available in three different options: the Standard Glove, protecting the whole hand, the Palm Trigger and the Index Trigger, that can be used alone or in combination with other types of glove and can be triggered with different mechanisms respectively on the palm, by the middle finger, or by the index. This component is what really fuelled the idea, as the founders stated, because the advantages of a smart glove are two-fold. Firstly, workers always use gloves while performing their tasks, often for safety reasons, and these functions could be enhanced with a computational core; secondly, the hands are what touches, senses and controls the production process, and also all these abilities could be aided by technology that fits the hand perfectly [207].

Thus, what really makes the difference is the combination of such tool with its computational core. The MARK ONE S is a small device that can be embedded in the fabric, equipped with a rechargeable battery, a scan able to identify 1D and 2D bar codes and many other sensors for heat, weight and even energy units[208].

The MARK 2 edition, released in 2019, brings the flow of data to a whole new level as it can also be connected to smart devices such as tablets and wearables, other than to all the other gloves, This is allowed by the BLE (Bluetooth Low Energy) technology, contrary to its predecessor that was only using radio channels. Other newly added features are an extended battery and long scan ray.[209]

The main tasks in which the glove is used are divided into four main categories: Picking, Assembly, Packing and Staging. Through all these phases of the production process, the tool allows a high level of efficiency, thanks to his ergonomics, and of speed and security. In fact, the glove has a Worker Feedback System, that not only stores the information created by the worker, but also makes available the general system information and responds to the actions of workers, confirming whether the task was performed correctly or not through vibrations and signals. The principal industries currently employing the glove are the automotive, retail, logistics, aviation and manufacturing ones.

---

207 Retrieved from https://www.youtube.com/watch?v=jTHL26WCrL0
208 Retrieved from https://www.proglove.com/products/markones/
209 Retrieved from https://www.proglove.com/products/mark2/

3.1.1 The wearables industry and personal data

Although the advantages arising from the use of the smart glove are undeniable, some shortcomings need to be considered too. As shown in the previous paragraph, like many other Industry 4.0 applications, the ProGlove relies on data a lot. They are not only the output of the tasks carried out by the employee, but also the inputs, as they guide him through the job thanks to the feedback system. Once again, one may think that the only type of crime that can impact on those data is industrial espionage or in general, cybercrimes. However, the ProGlove produces also many personal data. As the authors of the Directorate's document observe, these might be the location of the worker, his habits and his performance[210]. So far, this case may just seem an ordinary situation in which personal data are collected and stored in an ambiguous way, of which the subject may not be fully aware, because of the ubiquitous technologies that surround us. However, some peculiarities could have triggered the need, for the authors, to state that individuals should reassess the power over their data specifically in the Industry 4.0 context. One reason might be the fact that this specific tool is both created and used in this environment. It is the product of advanced technologies, cyber-physical systems and sensors and, at the same time, it helps the end-users implementing the intelligent manufacturing: it is both the input and the output of the Smart Factory. Another interesting aspect could be related to how blurry becomes the line between what if physical and what is computational when it comes to tools such as the glove, i.e. tools that are commonly known as wearables.

A wearable device is commonly defined "as a material product, specifically a garment or accessory worn on the body that is inspired by, created through, or enhanced by digital or electronic technologies"[211]. The wearable industry is older than it seems, however its real development is linked to the spread of ubiquitous technology. The first consumer wearable device can be traced back to the 1970s and it is the HP 01 calculator watch, followed by Casio databank watch, now commonly recognised as a landmark of the industry[212].

An important aspect of the wearables industry is the distinction between Wearable Computers and Smart Textiles. The former refers to electronic devices embedded in a fashion item such as a bracelet or watch, that allow users to make the most of the

210 Gouardéres, F., 2016
211 King, M., 2011, p. 8.
212 Page, T., 2015.

technology in a discrete and unobtrusive way. Smart Textiles' abilities instead come from the inclusion of sensors and electronics directly in the fabric, that becomes able to sense what is around it. Smart Textiles have a reduced range of interaction possibilities with the user, but can be worn for longer times and satisfy higher aesthetic requirements[213]. The ProGlove could be seen as an integration of both technologies as the glove represents the Smart Textile, made of fabric and endowed with sensors, covering the whole hand. While the computational core (MARK or MARK2) is the Wearable Computer. After some years of increasing sales, the release of Wearable Computers started to have a slowdown. As Page reports, according to many scholars, this was caused by the rise of smartphones, that caused people to discard devices that could only execute one function[214]. A textual analysis carried out by Martin shows very precisely how the number of papers analysing Wearable Computers and smartphones changed in the last years, with a drastic shift in 2007, when the Apple IPhone was released[215]. The same did not happen to Smart Textiles, as they are "used for monitoring physical activities in ways which smartphones are unable."[216]

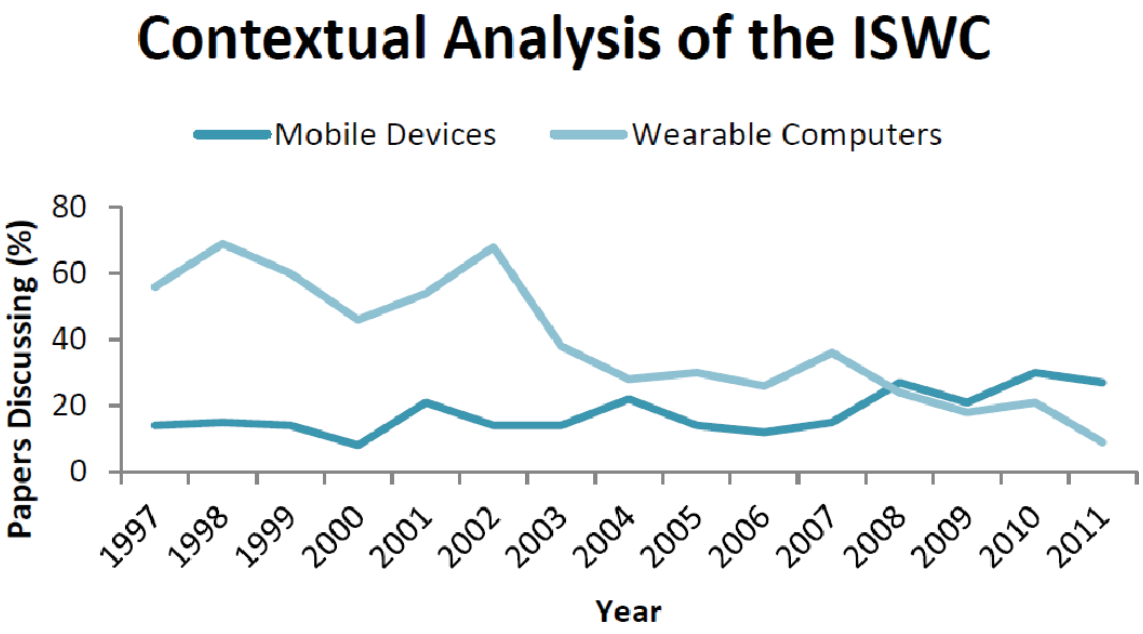

Figure 8: Contextual Analysis of the ISWC (source Martin, A., 2012, quoted from Page, T., 2016)

213 Ibidem.
214 Page, T., 2016; Smith, D., 2007; Buenaflor, C., & Kim, H., 2013.
215 Martin, A., 2012.
216 Page, T., 2015, p. 16.

However, the situation has been changing again in the last years, leading to new unexpected growth. According to CCS Insights, a market intelligence and advisory specialised firm, the wearables market was going to treble in the years from 2014 to 2019, to reach the over $25 billion worth and the sale of more than 245 million devices[217]. According to the IDC report released in March 2019, only in the last quarter of 2018 the worldwide wearables market grew of 34%, while the growth for the whole year was 27,5% reaching 172,2 million wearables shipped. Regarding the different types of tools, IDC confirmed that smartwatches are the most popular ones. They grew 54,3%, constituting 29,8% of all wearables shipments in 2018. However, the most surprising growth was that of ear worn devices, that equalled 66,4%, making the 21,9% of the market. According to Jitesh Ubrani, senior research analyst for IDC, this can be explained by the fact that many smartphones producers are removing the traditional earplug jack from their devices[218]. Also, future forecasts show that this market is set to another astonishing growth, reaching the value of $51 billion by 2022, with eyewear and headwear being the fastest-growing products[219]. Finally, from all the afore-mentioned reports, it results that the US is the principal market for wearable devices and so will be in 2022.

Although the slow-down of the wearables market suggested by Page did not come true, an interesting insight appears in his research. To find motivations that could justify the decrease in sales that was forecasted, the author analysed consumer preferences too, showing that according to the TNS research, the second biggest barrier to purchase a wearable device is privacy concerns, only preceded by price[220]. Although a more recent report from Price Waterhouse Coopers later showed that the privacy barrier went even decreasing in the following years, privacy concerns are still worth being analysed[221]. As it was shown earlier, the smart glove as a tool that belongs to the wider industry of wearables, was the starting point for the proposal of an Industry 4.0 Bill of Rights. The

---

217 Retrieved from https://www.ccsinsight.com/press/company-news/2332-wearables-market-to-be-worth-25-billion-by-2019-reveals-ccs-insight/

218 Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS44901819&utm_medium=rss_feed&utm_source=Alert&utm_campaign=rss_syndication

219 Retrieved from https://www.bloomberg.com/press-releases/2019-07-01/wearable-technology-market-growing-at-a-cagr-of-15-5-and-expected-to-reach-51-6-billion-by-2022-exclusive-report-by

220 Page, T., 2016; Transparency Market Research, 2013.

221 Pwc, 2016, p.5.

European Data Regulation framework, analysed in the previous chapter, shows how laws kept adapting to increasingly advanced technology, from the augmented presence of the internet to the spread of mobile devices and how they fully merged with the daily life of people. The difference of wearables, is that they do not only represent the merging of mobile devices with daily lives, but with individuals, their clothes, their bodies and their health. The result of this is the creation of a new identity, the quantified self, and of an unprecedentedly wide set of personal and sensitive data.

"Imagine waking up in the morning-your Fitbit alarm silently buzzing so you don't oversleep. They know you had a restless sleep. You get dressed and decide to walk to work. They know where your office is located. So far, you burned approximately 250 calories. They know you walked 4000 steps. After work, you rush to the gym and get there just in time for your favorite spin class. They know you entered Equinox at 7:20 p.m. After a full day, you haven't reached your goal just yet-15,000 steps. So, after dinner, you decide to take your dog for a long walk until your Fitbit buzzes again, letting you know you reached your goal. You are one step closer to living a healthier lifestyle and they know it. But who are "they?""[222]

3.1.2 The quantified self: social and privacy concerns

The concept of the quantified self was already introduced in chapter one and it refers to the result of the habit of tracking physical, health and body-related data and analysing it in order to optimise one's behaviour. It is important to notice that, in the general wearables literature, the quantified self often represents only a category of wearables, separate from others[223]. Regardless of categories, as Jülicher and Delisle point out, what really matters is that wearables keep becoming more discrete and body integrated. In fact, the authors report that tools that would belong to other categories than the quantified self one are already able to track health and body-related data.[224] The same assumption is valid for the smart glove too, because alike these other tools, it could potentially track all sorts of sensitive behaviours from which privacy risks arise.

All in all, the quantified self, and the technologies that make its existence possible, are very difficult to deal with, as the relationship between the benefits and risks arising from the collection of such data are in deep contrast and produce not only legal but social implications. In an article written in 2017, Sharon describes three principal dichotomies between advantages and disadvantages deriving from the use of wearables and the

[222] Troiano, A., 2016, p. 1715.
[223] For example, in the aforementioned CCS report, the categories of wearables are: Smartwatches, Quantified Self, Wearable Cameras, Professional Sport, Healthcare, Emerging wearables, Virtual and Augmented reality.
[224] Jülicher, T., Delisle, M., 2017

emerging of the quantified self[225]. The first one refers to the contrast between empowerment and surveillance. When the individual uses wearable devices to track himself, he is somehow called to action and to gain a deeper understanding and control of himself and his body: "users are called upon to 'take control of your sleep', 'eat smarter', and 'tell your weight who's boss', and devices are depicted as facilitators that can 'help you on your quest [toward glucose control]'"[226]. As a consequence, many scholars even advocate that, thanks to self-tracking, the healthcare sector (one of the most important in the wearables market) is set to become more democratic. Those who take control over their behaviour by collecting data about their sleep, diet and physical activity will somehow gain an ally in the conversation with their practitioners, making the relationship between doctor and patient a bit less asymmetric. In general, the quantified self allows individuals to shift from being a passive citizen to an active one. Moreover, one of the peculiarities of tools and platforms that allow self-tracking is that the process of data collection is continuous, therefore the profile of the individual that results from that is much more detailed and articulated, allowing a very high degree of personalization of the service and experience.[227] The positive effects generated by empowerment and personalization, is contrasted by surveillance. Although more will be written on this topic in the next pages, in the specific context of wearables and of the quantified self, what is especially alarming is that, while surveillance was usually something imposed from above, now it is not anymore. This can be explained by the fact that modern apps and the way in which wearables are structured, make tracking feel like it is a game, in which it is even possible to compete with others. In this way, users do not understand how intrusive this behaviour is[228].

Another contrast in the discussion on wearables and self-tracking is the one between "greater (self-)knowledge [and] reductionism and the non-impartiality of numbers"[229]. The data produced via wearables by the quantified self are increasing in number and, as it was argued before, they allow individuals to have a high degree of personalization in the services they receive and of comprehension of themselves, their activities and behaviours. In other words, wearables produce knowledge, both for their users and, in general, for those who access those data. The main manifestation of this belief is given

225 Sharon, T., 2017.
226 Ibidem, p. 97.
227 Ibidem.
228 Ibidem.
229 Ibidem, p. 102.

by the Quantified Self Movement, that chose the formula "Knowledge through numbers" as its motto[230]. However, as the critiques to this approach argue, often an excessive trust in data and quantification can lead to a distorted and incomplete view of reality. Very often in fact, algorithms and data use symbols and indicators that only approximate the real values that are being measured, in order to translate them to numbers. Of course, when it comes to very relevant, sensitive and variegated subjects such as health or the employees' performance, the resulting picture could end up being even far from accurate[231]. Especially in the case of healthcare, very often this trust in data only makes the line between the accuracy of predictions and surveillance blurred. Modern platforms ask their users to provide data that are not related to health or the body too, such as social media posts and activities and credit card purchases, with the excuse that this type of information will make the patient's profile more complete. However, what is really happening is that the user is willingly providing to those who work on these apps with a whole set of sensitive data that are going to be used in a way the users do not fully understand.

3.1.3 GDPR and wearables

Assuming that individuals must reaffirm their rights over their data with a new tool, such as a Bill of Rights, is also like assuming that the legislative framework in charge of the protection of data that is in place is not sufficient. As a consequence, the question of whether General Data Protection Regulation grants sufficient protection against the risks of wearable devices will be answered in this paragraph. Montgomery, Chester and Kopp observe that under many aspects the GDPR shows real progress in ensuring protection against many of the risks that could be caused by wearable devices, but there are some limitations too[232]. Starting with the advances, many of them refer to the fact that the type of data that wearables can collect very often fall under the classification of "special category", i.e. sensitive data, the processing of which is generally prohibited. Especially in the case of those wearable collecting health-related data, all the information gathered basically is considered sensitive data. In fact, the category also includes "a number,

230 Retrieved from https://quantifiedself.com
231 Sharon, T., 2017.
232 Montgomery, K., Chester, J., Kopp, K., 2016.

symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes"[233]. This has an impact on processing too, as according to GDPR, automated decisions should not be based on sensitive data, unless the special requirements for the processing of such data are met and special safeguards are in place too. Special categories of data are also additionally protected when processed on a large scale, as data protection impact assessments were made mandatory in such circumstances. Finally, another important principle that was introduced with the GDPR which becomes extremely important when it comes to wearable devices is the right to data portability, that means that the data subject can obtain his data in a comprehensible form from the data controller and move them to another one.

However, the GDPR shows some challenges too. One of them is the set of derogations to the prohibition of processing special categories of data, that seems to be expanded, even in the case of health-related data. Derogations include preventive medicine, assessment of the capacity of employees, diagnosis and the provision of healthcare. Finally, other problems arise with the derogations relative to public interest matters. Both the further processing of data prohibition and the data storage limitations are derogated when it is justified by scientific, historical and research purposes.

3.2 The Internet Bill of Rights

3.2.1 Identifying a Bill of Rights

In the document written by the Directorate for Internal Policies of the European Parliament, the tool suggested to allow people to reaffirm their rights over data in the Industry 4.0 context is a Bill of Rights. As reported in the document, the idea is rooted in the proposal, launched by a firm called Pachube, of creating an Internet of Things Bill of Rights with the same aim[234]. It is interesting to notice how, while the proposal of an Internet Bill of Rights stimulated dialogue and ideas, especially in the United States, the Industry 4.0 Bill of Rights was not given much attention, neither from the lawmakers, nor from businesses. In any case, the first step to understand the validity of such proposal is to discern how such a tool is different from what already exists. For this task, the recent literature about Internet Bill of Rights could be the right starting point.

[233] GDPR, 2016, (35).
[234] Gouardéres, F., 2016.

As it was previously introduced, the first example of an Internet Bill of Rights was launched by Pachube in 2011, a firm that offers to companies innovative solutions to connect their tools and devices in the Internet of Things. The business model relies on a Cloud platform in which clients can connect products in an efficient and fast way and monitor the data they produce. After 2011 Pachube was acquired by LogMeIn, which recently sold it to Google. After that, the firm rebranded and changed its name to Xively[235].

The principles of the Bill of Rights written by Pachube are as follows:

"1. People own the data they (or their "things") create.
2. People own the data someone else creates about them.
3. People have the right to access data gathered from public space.
4. People have the right to access their data in full resolution in real-time.
5. People have the right to access their data in a standard format.
6. People have the right to delete or backup their data.
7. People have the right to use and share their data however they want.
8. People have the right to keep their data private."[236]

Neither in the US nor in Europe the discussion on such a proposal was systematic. However, it is undeniable that it drew attention from institutions and lawmakers. The second pioneer after Pachube was Italy, that in July 2014 created a parliamentary commission and opened a debate aimed at writing principles that could protect the individuals from the internet with a constitutional methodology[237]. One year later, the Commission approved the text of the Bill of Rights and on the 3rd November 2015, the Camera approved a motion that commits the Government to promote the principles and their enforcement at a national and European level[238].

In the United States, instead, there have been very recent developments in this direction, as congresswoman of the Democratic Party Nancy Pelosi, gave to Ro Khanna, the representative of the district in which Apple, Yahoo and Intel reside, the task to write an Internet Bill of Rights to create a healthier internet environment[239].

---

235 http://www.iotinsights.com/governance/deals-and-finance/logmein-acquires-pachube/ ; https://xively.com

236 Gouardéres, F., 2016, p. 77.

237 Retrieved from https://st.ilsole24ore.com/art/tecnologie/2014-07-20/internet-bill-of-rights-italia-081243.shtml?uuid=ABS0iecB

238 See https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/note_informative_2017.pdf

239 See https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html

The ones reported above are exclusively examples of Internet Bills of Rights. The general discourse about regulating the environments created by new technologies has different approaches, for example regulating only some specific aspects of the Internet of Things. As a consequence, other types of Bills of Rights were created, such as the Bill of Rights of the Users of the Social Web and the Social Network Users' Bill of Rights[240].

However, for how different the ideals, the processes and the authorities that carried out the dialogue on such tools are, what must be understood is what distinguishes them from the legal frameworks employed today. In other words, it is necessary to identify the features of Bills of Rights.

It is not easy to define a Bill of Rights. Frank I Cobb, American journalist described them as follows:

"The Bill of Rights is a born rebel. It reeks with sedition. In every clause, it shakes its fist in the face of constituted authority."[241]

A more detailed description was made by Philip Alston, a law professor at the New York University and expert of Bills of Rights, who instead of providing a definition, identified three main features that such documents should have. They can be summarized as:

1. The protection of significant rights
2. The ability to be binding for the government
3. Redress, in case of right violations[242]

Moreover, while the afore-mentioned points are rather related to the content, some other aspects should be discussed, what should be the territorial scope of the document and what authorities should work on it[243].

3.2.1.1 The protection of significant rights

This feature seems to be the most obvious one, as Bills of Rights were born as declarations aimed at protecting fundamental rights and human liberties. However, this is also the main source of complexity relative to such documents. Acknowledging and creating a right has infinite social, historical, economic and cultural implications. As Musiani reports, this can be explained on two levels[244]. The first one is related to the oldest paradox

240 Klug, F., 2007.
241 Quoted by Klug, F., (2007).
242 Ibidem.
243 De Minico, G., 2015.
244 Musiani, F., 2009.

regarding rights and the law, as the existence of fundamental rights and their value through time cannot be explained. Neither can the logic behind the rights nor their essence. But still, somehow through history, rights that protect the individual were created and recognized as extremely important. The second level is that recognizing a right is especially difficult due to differences between nations, cultures and social realities. This is why, coming to the recognition of a value is the result of historical processes, that may vary across people, countries and religions. Of course, applying such discourse to the Internet could be even more difficult, due to the intrinsic ineffable, borderless and diverse features of this environment. The Internet is by definition an open space, aimed at sharing opinions, ideas and all sort of contents, in which people from opposite sides of the globe can get in touch. As a consequence, the process leading to the creation of core rights that protect the individual in this environment is no easy task. However, this does not mean that it is impossible. One strategy towards a Bill of Rights of the Internet, as suggested by Gill, Redeker and Gasser, could be simply extending basic rights to the internet environment[245]. In fact, the literature regarding Internet Bill of Rights often shows this underlying process, as many of the rights are some of the liberties enshrined in national constitutions and international treaties. One example is the protection of freedom of association on the Internet. Other rights instead seem to be new, i.e. the right to be forgotten, but they root in traditional concepts such as personality rights[246].

3.2.1.2 The ability to be binding for the executive

This feature is fundamental as it is related to the legitimacy of an instrument such as a Bill of Rights. This requirement is in place when "Governments, like the courts and all public authorities, are explicitly prohibited from acting incompatibly with the rights it [the Bill] upholds"[247]. As Klug explains, this feature can be justified by the fact that a Charter of Rights is somehow a higher law, to which other lawmakers have to adjust. However, sometimes a balance has to be found between the fundamental character of Bills of Rights and their ability to shut down national governments, as this could lead to a democratic deficit, which is typical of these instruments:

245 Redeker, D., Gill, L., Gasser, U., 2009.
246 Ibidem.
247 Klug, F., 2007, p.8.

"the power to determine the meaning of broad values like liberty or privacy – and to re-write or repeal laws which don't conform to that meaning – are handed from elected politicians to unaccountable judges who effectively become legislators in the process."[248]

3.2.1.3 Redress in case or rights violations

When it comes to fundamental rights, redress is a powerful instrument necessary for their respect and as such it has to be granted. According to Alston, this is the last feature of a Bill of Rights. It is easily recognized that instruments that concern with fundamental rights have to allow redress. The mode in which redress should be carried out is not specified by Alston and it varies from case to case. Different types of limitations and circumstances can discipline this right. One example is the European Court of Human rights, that in Article 13 of the Convention declares that "everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity"[249]. Article 35 instead states that before a matter is brought to the Court, all domestic remedies have to be exhausted and less than six months should have passed after the final decision. This is a very important clause, because it implements the principle of subsidiarity in a way that the workload of the Court is reduced and made easier, as a very detailed examination is granted by the time the issue reaches the Court[250]. Another advancement to the right to redress of the European Court of Human Rights has been recently reached, as Europe is working towards collective redress, that would allow a group of people to go before the Court when there has been a case of a mass harm. In these situations, in fact, usually the process is extremely lengthy and costly when individuals decide to go to trial alone. However, so far only a draft report has been published regarding the possibility to allow collective redress for consumers.

248 Ibidem, p.10.
249 ECHR, Article 20.
250 See https://www.echr.coe.int/Documents/Pub_coe_domestics_remedies_ENG.pdf

3.2.1.4 Authority, scope and structure

Although the most important features to define and identify a Bill of Rights were the afore-mentioned ones, other important issues are discussed regarding the characteristics that such an instrument should have. The first one is the equilibrium between regulation and self-regulation. In the document from the Directorate of the European Parliament, when proposing a Bill of Rights of Industry 4.0 inspired by the Internet one, the author refers to the efficiency and effectiveness of self-regulation[251]. Self-regulation refers to when a body or entity group of people voluntarily commits to a set of rules that is not promulgated by an external authority. However, most scholars agree that the solution is not an *aut aut.* On one hand, it is recognized that the State cannot have the monopoly over regulation, as it would be the most expensive solution. Private parties know their needs better than the State and can therefore adapt rules to them. Moreover, especially in a context such as the one of the Internet and new technologies, the State could not keep up with the fast pace of these changes. On the other hand, self-regulation should not be let without boundaries. The opposite effect could take place, as laws would probably come to only represent private interests and private parties cannot always guarantee transparency and accountability[252]. According to De Minico, this situation can be defined as the independence model and it refers to when the State leaves decisional power to private bodies and only intervenes when regulation is missing, but when it is not required it generally does not intervene[253]. A solution that entails negotiation and collaboration between the State and private parties is thus necessary, in a way that "the State entrusts meaningful social tasks to a private body while continuing to regulate the overall legal structure and decision-making process."[254]. Thus, there should be a hierarchy in which self-regulation is a secondary tool, after the law. The role of the State should be that of an architect, that does not try to define individual behaviour, rather than a general structure. Finally, the State will intervene in case of deviations from this structure[255].

Another debate concerns the choice of the authority that should be vested with the power to create the Bill. It is common that supranational entities are usually in charge with the creation of Charters that protect basic rights, due to the a-territoriality of the rights they

[251] Gouardéres, F., 2016, p.78.
[252] Redeker, D., Gill, L., Gasser, U., 2009 p.5; Gouardéres, F., 2016, p.78.
[253] De Minico, G., 2015.
[254] Ibidem, p. 5.
[255] Ibidem.

concern. Another reference can be made with regard to the European Convention on Human Rights, as in that case Europe is legitimated by the Member States to be the guardian of Human Rights. Of course, in the case of an Internet Bill of Rights the situation would be a bit more complicated. As De Minico points out, the participation in the writing process of one or more States should be definitely be rejected, in favour of a supranational body. The explanation is the same as for fundamental rights. The Internet is a-territorial per se and an authority constrained by national boundaries could never ensure a sufficient level of protection[256]. Also, letting international bodies write it would generate the same results, because very often they are influenced by one State and they reproduce, on a different scale, the dynamics of international politics. An alternative solution could be letting the people write their own Internet Constitution, as in this way there would not be limitations to its powers and scope. However, then the problem would be the same as before, in the choice between hard law and self-regulation. The solution should be similar too. Previously it was suggested that self-regulation should only be a secondary tool, while the State should define the architecture of the Bill or Charter. What was previously generally defined as a State should be a "supranational authoritative body"[257], that has to be in a constant dialogue and negotiations with all the stakeholders representing the different private interests that concern the internet, such as "entrepreneurs, web surfers and consumers"[258].

Finally, there are some last criteria that can be used to identify a Bill of Rights. They pertain to the content and to the way the lawmaker's powers can be limited, which is fundamental when basic rights are at stake. Once again, reference is made to the European Court of Human Rights, as these requirements are often recalled in the European Convention and they constitute the foundation of European law: necessity, proportionality and indispensability[259]. These measures are fundamental for a Bill of Rights, because they represent limitations to the power of the policymakers, helping in the construction of an equilibrium between regulation and self-regulation. Necessity is the requirement that has to characterise those circumstances in which a fundamental right is derogated. In other words, if sacrificing the right is unavoidable, then it will be possible to do so. Moreover, there is a limit to the possible derogations too, thanks to the principle

256 De Minico, G., 2015.
257 Ibidem, p. 22.
258 Ibidem.
259 Ibidem.

of indispensability. The limit is set to the "minimum essential content", in a way that the right cannot be deleted completely. Finally, the principle of proportionality tests the appropriateness of the right: "Costs and benefits must be assessed in order to check that a proper balance has been found between the interests embodied in the protected rights and those on which the legislative restriction is founded."[260]

Although it is not fundamental to understand the implementation stage of the Internet of Things or the Industry 4.0 Bill of Rights proposal, another common aspect between these charters that is worth mentioning, is why such instruments are being chosen to reaffirm rights over new technologies. According to Celeste, these phenomena can be grouped in a general ideology that has been developing over the past few years, which can be described as digital constitutionalism[261]. The author believes that "contemporary society is experiencing a new constitutional moment"[262], because the circumstances in which people feel the need to exercise their fundamental rights have increased, due to the new threats posed by digital technologies. As a consequence, the constitutional ecosystem is reacting to this changed environment by creating a set of principles and rules that lead the response to these new challenges. This is why digital constitutionalism is not the response, but rather an ideology, that disciplines the different responses[263].

3.3 Scope and Value of GDPR

3.3.1 The GDPR as a Bill of Rights

As mentioned earlier, the Industry 4.0 Bill of Rights proposal, in the Directorate's document, seems to be not only the first but also the last time in which the creation of such an instrument is suggested. On the contrary, the Internet Bills of Rights proposal keeps on stimulating research and discussion. Thus, behind analysing the features that such a document should have, it is necessary to understand if it is needed. Another interesting factor is that the Directorate's document was written and published in 2016, the year in which the European Parliament and Council agreed on the text of the GDPR. Thus, it is natural to wonder whether GDPR is the type of tool the authors were wishing

260 Ibidem, p. 25.
261 Celeste, E., 2018.
262 Ibidem, p. 3.
263 Ibidem.

for when writing the document. To answer this question, it will be necessary to see if the features that define a Bill of Rights can be found in the GDPR.

The main features that define a Bill of Rights according to Philip Alston are the protection of significant rights, being binding for the executive and the possibility to redress[264]. Starting from the latter, we can assess that the GDPR definitely offers remedies in case of violations. These instruments are actually very advanced and constitute some of the main novelties compared to previous regulation. In fact, the GDPR led to the creation of an authority, i.e. the European Data Protection Board, that is divided into many local Data Protection Authorities (DPAs), one for each Member State. The first thing, that the individual who sees his rights to data protection violated has to do, is to file a complaint with his national DPA, which has three months to conduct investigations and then inform the individual with the results[265]. On the other hand, the individual has also the right to a judicial remedy against the processor or the controller, i.e. he can directly take action against the firm or organisation that violated his rights[266]. This process does not exclude the possibility to turn to the national DPA. Furthermore, if the DPA does not fulfil its tasks correctly, the individual can also file an action against the DPA.

Regarding the second requirement, i.e. being binding for the executive, the GDPR represents once again a dramatic advancement compared to previous regulation. Although the main focus is on businesses, also public authorities have their share of increased responsibility[267].

The first main change pertaining to them regards the Data Protection Officer (DPO). In fact, while for businesses the presence of a DPO is only mandatory when certain criteria are met, public authorities have to employ a DPO a priori: "The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity"[268].

Another fundamental change concerns the grounds for justifying the processing. In the Directive 95/46, one of the requirements for processing data was demonstrating a legitimate interest and this could be done by any processor or controller. With the advent

264 Quoted by Klug, F., (2007).
265 European Commission, 2016, Art. 77, 78.
266 Ibidem, art. 79.
267 Retrieved from https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-in-the-public-sector.html
268 European Commission, 2016, Art 37.

of the GDPR, legitimate interest is not a viable basis for public authorities to process personal data anymore, as stated in article 6.

"(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."[269]

Processing personal data for public authorities is still possible, but another ground must be found among those listed in article 6. Furthermore, also the principle of consent is not valid anymore to process personal data when the controller or the processor is a public authority. In fact, the GDPR recognizes that in that circumstance, given the imbalance of power between the individual and the public authority, consent could never be freely given.

"In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."[270]

Regarding the binding value of Bills of Rights, other observations were made in the previous paragraphs. Although they are not fully relevant to define the fundamental requirements, they give some insights on how a Bill of Rights should be. One of these observations concerned the equilibrium between self-regulation and the rule of law. It was proven that for such an instrument, the preferable solutions would be a combination between the two solutions, reinstating the primary value of a lawmaker authority and the secondary value of self-regulation. All this should happen while keeping negotiations with private parties open, in order to take into account all the possible interests that should be represented. The General Data Protection Regulation seems to meet this requirement too. In fact, as Segovia Domingo and Desmet Villar point out, the GDPR is a good example of co-regulation[271]. Co-regulation was defined by the European Union as a mixture of a basic legislative act and voluntary agreements between the parties concerned aimed at respecting the legislative act[272]. The GDPR aims at reaching this equilibrium, by encouraging firms to stipulate codes of conduct that show compliance to the regulatory rules laid down by the European Union.

---

269 Ibidem, Art. 6.
270 Ibidem, (42).
271 Segovia Domingo, A.I., Desmet Villar, N., 2018.
272 European Union, 2011.

The last fundamental criterion identified by Alston that should characterise a Bill of Rights is the protection of fundamental rights. Also, this criterion is met as data protection is recognized by the European Union as a fundamental right as in Article 8(1) of the Charter of Fundamental Rights of European Union and Article 16(1) of the Treaty on the Functioning of the European Union.

Although from this analysis the question asked in this paragraph seems to be answered already, for the completeness of this research also the structure prerequisites will be traced in the GDPR. Regarding the authority that should have the power to create a Bill of Rights, it was stated that it should be a supranational authority that is able to negotiate with private parties. Of course, the supranational authority requirement is met as the European Union is one. A bit less is known about the dialogue with European businesses and consumers, especially in the drafting process. However, the European Commission is constantly monitoring the degree of comprehension and acceptance of the GDPR amongst businesses and consumers, as their Eurobarometer survey shows[273].

Finally, the last criteria that have to be checked are the structure criteria: necessity, indispensability and proportionality.

The respect of necessity and proportionality is strictly related. In the case of data protection, the necessity requirement is met when limiting the right to data protection is necessary "for an objective of general interest or to protect the rights and freedoms of others"[274]. One example pertains to the EDPS opinion 3/2016 on the European Criminal Records Information System's proposal to facilitate the exchange of information of third-country nationals with the aim of the fight against crime and terrorism. In the proposal, it was suggested that also biometric data were included in the information, in order to ensure the identification of the individual. However, the EDPS stated that there are other means to reach this aim than the inclusion of fingerprints, which therefore was not necessary[275].

The proportionality principle, which is secondary to the necessity one, refers to the appropriateness of a measure. In the case of data protection, the requirement is met when "advantages due to limiting the right are not outweighed by the disadvantages to exercise the right"[276]. One example always pertaining to the EDPS opinion 3/2016 is the proposal

---

273 Available at https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_19_4449/IP_19_4449_EN.pdf

274 Retrieved from https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf p. 2.

275 Ibidem.

276 Retrieved from https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

of allowing access to the convictions of third-country nationals with the aim of the fight against crime and terrorism. Of course, this measure was deemed as proportional, as the benefits arising from the protection against such risks compensate for the disadvantage of the limitation to data protection[277].

Of course, the assessment of necessity and proportionality varies from case to case and the legislator is responsible for this task, as stated in the Toolkit of the European Data Protector Supervisor. In any case, the principles of necessity and proportionality are principles that are fundamental in European law, therefore it is impossible that a European legislative tool does not respect that. However, what can be checked is whether GDPR contributes to the respect of these principles itself. For what concerns necessity, the GDPR lays down the aims for which interfering with the right to data protection is legitimate[278]. Furthermore, GDPR states that for those types of processing of personal data that could generate a very high risk for the data subject, an impact assessment has to be carried out, including a necessity valuation[279]. Regarding proportionality, the GDPR respects and encourages that principle too.

In fact, other than specifying that an impact assessment is needed for the processing of data that could generate a high risk for the subject, the GDPR directly states that the protection of data is not an absolute right and therefore it has to be balanced with other fundamental rights, such as freedom of thought and religion, according to the principle of proportionality[280].

As it was proved in the previous lines, the GDPR seems to have all the requirements to be defined a Bill of Rights. Not only the prerequisites identified by Alston were traced back, but also the features that should characterise the structure of a document that falls under the umbrella of digital constitutionalism.

3.3.2 Is an Industry 4.0 Bill of Rights still necessary?

At a first glance, it seems like this question has been answered: by demonstrating that the GDPR can be defined as a Bill of Rights of data protection, it was also proved that such

277 Ibidem.
278 European Union, 2016, Article 23.
279 Ibidem, Article 35.
280 Ibidem, observation (3).

an instrument is not necessary. However, it is necessary to consider that there might be other interpretations of what the authors of the Directorate's document wrote.

The first requirement of a Bill of Rights according to Alston, is that it has to protect fundamental rights. In the second paragraph of this chapter, some examples were made on how to adapt this requirement to a digital context. The suggested strategy was to extend fundamental rights to the new context (ex. Freedom of association should be granted on the Internet of Things too). It is obvious that the scope of the GDPR only includes one fundamental right, i.e. data protection, which means that it can be identified as a Bill of Rights of data protection, but surely not as an Industry 4.0 Bill of Rights. Such an instrument would have to be created from scratch, possibly respecting the requirements mentioned in the previous paragraphs and understanding whether it is necessary or not, the question whether Industry 4.0 needs to be regulated per se would have to be answered. In other words, do freedom of thoughts, of religion and of association need to be reaffirmed in the Smart Factory context?

Instead, the authors of the Directorate had a very specific objective in mind, that was creating a Bill of Rights that gives the opportunity to *control data* in the Industry 4.0 context. Such an idea was inspired by the creation of a very intrusive tool, i.e. the Smart Glove, that, as demonstrated in paragraph one of this chapter, belongs to a market that is destined to grow exponentially in the next years, posing unprecedented problems for data protection. Thus, if the latter is the right interpretation of the Directorate's document, what the authors were wishing for is a Data Protection Bill of Rights that can increase protection levels in the Industry 4.0 context.

The last observation concerns once again the GDPR. Although it was demonstrated that an Industry 4.0 Bill of Rights per se is not necessary, this does neither mean that sufficient tools for the protection of data in such context are already in place, nor that the GDPR cannot be improved in that direction. In fact, one solution could be to simply suggest some improvements, aimed at making the GDPR (or some of its aspects) more Industry 4.0 specific and ensure the degree of data protection that the Directorate refers to.

3.4 Improving the GDPR: employees of the Smart Factory

As recalled many times in the last chapters, the protection of personal data in the Smart Factory does not always appear obvious. The common understanding of the type of usage

of data in this environment concerns mainly production and, in general, supply chain data. In paragraph 2.1.3 of chapter two, it was demonstrated that also personal data are very relevant in the Smart Factory. However, there is one more distinction to make in the Industry 4.0 data context, and it concerns the data subjects. In fact, not only customers share many data in the process of smart manufacturing or smart maintenance, but also employees. In other words, the challenge of personal data protection in Industry 4.0 exists along the data-customer nexus and along the data-employee[281]. In the next paragraph, the focus will be on the second nexus.

3.4.1 Employees surveillance practices and tools

As Moeller points out, the need to deal with the protection of employees' personal data rises from the very essence of the Smart Factory and Industry 4.0. In fact, the business model of this environment relies on the implementation of remote working, especially supported by virtualisation, that allows the creation of many data itself.[282]

In turn, different degrees of intrusiveness can be distinguished. Remote working is very common nowadays and can be found almost in every workplace. Tools and methods such as video conferences and smart working models are of course a threat to the privacy of employees, but can be still controlled. However, in a Smart Factory context, remote working can become much more intrusive, due to the special link established between men and machines all along the supply chain. Thanks to Cyber-Physical Systems, very often workers do not need to get physically in contact or even close to the machines they use or produce, allowing new effective systems, such as remote maintenance, but also threatening their own privacy. The next degree of intrusiveness is the dramatic increase in the surveillance of the workplace, that is caused by the spread of wearable devices, such as the Smart Glove.

The topic of surveillance in the workplace has always existed all over the world and according to Ball, it goes hand in hand with corporations. An interesting aspect, according to the author, is that very often the term surveillance is used as a synonym of monitoring, while in fact, these two practices can both have negative and positive consequences, but have very different connotations to different audiences[283]. In fact, Ball notices that a

281 Moeller, C., 2016.
282 Ibidem, p. 155.
283 Ball, 2010.

dystopian character is often attributed to surveillance and the scholars who write about this topic "are concerned with power, politics, resistance and meaning-making by employees under surveillance"[284]. On the other hand, those who write about monitoring do neither consider the dystopian character, nor the social and political implications of it. Of course, monitoring relies on the data that the advanced IT systems can collect and process and can be the source of competitive advantage. Thus, the worker somehow expects to be monitored. However, the practices that are being employed become more and more intrusive and this can lead to negative consequences too. A very recent report identifies four different monitoring practices or instruments, that can lead to severe downturns: Prediction and Flagging Tools, Remote Monitoring and Time-Tracking, Gamification and Algorithmic Management, Health and Biometric Data[285].

Prediction and Flagging Tools

This practice refers to the use of technologies that aim at flagging some behaviours of employees and in general, at predicting their future characteristics. According to McKinsey, thanks to AI a new form of warfare has emerged: the talent war. In fact, very basic risk score assessments, such as drug testing or checking criminal records, are now assisted by very advanced predictive tools. Especially in the hiring process, digital interviews are increasingly used, in order to control and value the tone, linguistic skills and emotions of the candidate. With such a method, the hiring manager can then compare the interview to samples, derived from high-performing employees, and decide whether the candidate is attractive or not[286]. As Mateescu and Nguyen report, increasingly sophisticated tools are being created to scan social media posts of candidates. Predictim is a recent one, the success of which was determined by the increased demand from companies for such an instrument[287]. When the hiring process is over, predictive tools keep on being used, especially to analyse how employees feel and act. This is especially important to increase productivity and employee retention. When companies are able to see if their workers are unhappy, or low-performing, they can understand what causes these behaviours and then change it. As Davenport, Harris and Shapiro report, Google conducted an analysis of its under-performing employees and found out that they were

284 Ibidem, p. 88.
285 Mateescu, A., Nguyen, A., 2019.
286 Chamorro-Premuzic, T., Winsborough, D., Sherman, R.A., Hogan, R., 2016.
287 Mateescu, A., Nguyen, A., 2019.

either misplaced or badly managed. Sysco, instead, tracked the satisfaction of its employees and was able to improve the retention rate by 20%[288].

Remote Monitoring and Time-Tracking

As it was briefly introduced in the previous paragraph, the work environment is moving increasingly towards the virtual workplace and remote working. Along with that goes surveillance too. Nowadays, there is a number of software programs that allow employers to time-track their employees, by measuring how much time they spend on their computer and how. These trackers become increasingly sophisticated and detailed, for example Upwork, a freelancer software, has an additional tool that checks the number of keystrokes and clicks and screenshots the screen periodically. All these metrics end up in the so-called Activity Meter "that displays minute-by-minute data about a freelancer's work activity"[289]. Another system that is increasingly used for remote monitoring is telematics, which is the crasis between telecommunications and informatics, as it relies on data that are continuously streamed and received thanks to long-distance transmission. One example is the use how Uber employes this technology, as thanks to the GPS tracking of its cars and drivers, the company can analyse speed, acceleration and braking behaviour[290]. Uber implements this analysis for safety reasons, as the company affirms to be able to predict dangerous driving habits by checking on these metrics. However, with constant location and driving monitoring, the employee can be held accountable for every move he makes, including breaks, resulting in high pressure.

Gamification and Algorithmic Management

Algorithmic Management refers to "real-time data collection that feeds into automated or semi-automated decision-making and that is increasingly behind workplace scheduling, performance evaluations, and other decisions about workers"[291]. This phenomenon is typical in the sharing economy, as peer-to-peer interaction is very high and those tasks that are usually overseen by middle managers, can now be transferred to algorithms. One interesting case is that of Airbnb, that uses its algorithms for many different reasons, for example to determine how a house appears in the list when a guest is looking for one.

288 Davenport, T., Harris, J., Shapiro, J., 2010.
289 Mateescu, A., Nguyen, A., 2019.
290 See https://eng.uber.com/telematics/
291 Mateescu, A., Nguyen, A., 2019, p. 12.

This can depend on many things. Some are more obvious, such as the previous searches of the guest, his gender and age. Some others can depend on the behaviour of the hosts. In a study conducted in 2019, the authors show that there can be different ways of reacting to algorithms[292]. Only some people try to understand them and, when they can, they sometimes even manage to exploit the benefits they can offer. In general, however, that study proved that the underlying ambiguity of such algorithms generates, in the workers of our society, a deep sense of anxiety. The next level of Algorithmic Management is achieved when the real-time data obtained from the workers and the algorithms join together to gamificate the tasks of the employees. Gamification relies on human psychology that drives individuals to perform and strive for better results, in exchange for immediate gratification[293]. It can take place in many ways, from less to more advanced technologies. Some companies, for example, use electronic boards showing the score of employees in completing some tasks[294].

Health and Biometric Data

Finally, another surveillance practice is related to health and biometric data. The collection of such information is especially supported by the use of wearables in the workplace. This led to the introduction of wellness programs, that are usually justified with the offer of lower insurance premiums according to the step count, or with the optimization of the workplace, that will be healthier and funnier by adding a bit more competition. Of course, the pressure put on employees becomes very high, as in these circumstances, they feel obliged to insert data such as eating behaviours and medical records. Also, very often these technologies are used to monitor productivity as well and when comparison is allowed between the performances of different employees, they feel even more pressured by the fear to have some penalty or to be perceived as a liability[295].

[292] Cheng, M, Foley, C., 2019.
[293] See https://www.forbes.com/sites/danielnewman/2017/11/28/how-to-drive-employee-engagement-with-workplace-gamification/#553fec893cf0
[294] Mateescu, A., Nguyen, A., 2019.
[295] Ibidem.

3.4.2 Downturns of employees' surveillance

The issues raised by surveillance in the workplace are very complex, as somehow the benefits brought by these practices are considered an important source of competitive advantage. It is, first of all, a powerful tool for the protection against sabotage and data theft. Secondly, it allows monitoring and maintaining an appropriate level of productivity. Finally, it is an instrument that controls risk, as the results of the monitoring process can serve as evidence in case of legal actions.[296] However, in the same way as it is legitimate for employers to guarantee that productivity is maximised and that the workplace is safe and protected, in the same way employees have the right to privacy. This is not an easy conclusion, because in this way the workplace becomes a hybrid between a public and private space and the limit beyond which surveillance becomes too intrusive are very difficult to determine[297].

Some of the consequences of uncontrolled surveillance can be easily identified and result in severe threats and damages for employees. The first one is related to the already existent asymmetry between employers and employee. The negotiation power of the former becomes even greater as the latter does not have the opportunity to acquire the same amount and type of data of its counterpart. The difficulty of employees to cancel this asymmetry and to understand the criteria and methodologies of evaluation, in turn, results in a series of preventive behaviours. One of them is the fear of judgement, that inhibits employees' creativity. Other behaviours depend on the monitored tasks: when the workers find out that some types of duties are being controlled they tend to give them more attention. One last reaction is the so-called anticipatory conformity, that is caused by the importance given to quality over quantity. When the employees perceive that this is the message that the firm wants to send, they tend to act in a very disciplined way, in exchange of a real loss of interest and engagement in the task[298].

The second series of damages arising from excessive surveillance are strictly related to the invasion of the employees' privacy. Other than showing very often that the parameters assessed are not really useful in giving an overall valuation of a worker, many scholars believe that the data collected can lead to discrimination and social exclusion. A phenomenon that is spreading also in other fields than the workplace is that of the

296 Ibidem.
297 Moeller, C., 2016.
298 Ball, K, 2010.

"function creep", that refers to when "monitoring technologies can sometimes yield more information than intended, and management need to avoid the temptation to extend monitoring practice without consulting employees first"[299]. Of course, the risk of function creep is extremely increased when wearables are introduced in the workplace, as it gives employers the power to control very sensitive data too, such as health behaviours and social interactions[300].

3.4.3 What the Industry 4.0 data protection framework really needs

To have a detailed understanding of the extent to which these issues are a threat to privacy, it is necessary to understand where European legislation stands now for what concerns employees' privacy protection. As Moeller points out, the GDPR made some advancements in this regard compared to the Directive 95/46. The text of GDPR in fact, unlike its predecessor, contains an article dedicated to "Processing in the context of employment", in which it is stated that Member States should "provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context"[301]. Nevertheless, this advancement is probably not enough. First of all, it represents a step behind relative to the harmonisation efforts that took place in the past years, because by leaving space to Member States to act individually means that not all the countries will take action soon. Moreover, the resulting legislations will constitute a very diverse framework, undermining efficiency for European international companies[302]. Furthermore, such a situation would become even more complex, considering that it is not clear what kind of protection is needed and what issue need it, because some aspects of private communications are disciplined by the ePrivacy Directive, while in some countries monitoring work emails, for example, is allowed[303].

All in all, these matters are valid for workers in the digital era in general, but they are somehow exacerbated in the Industry 4.0 Smart Factory context, due to the increased interaction between men and machines and to the introduction of new technologies, such

[299] Ibidem, p. 90.
[300] Mateescu, A., Nguyen, A., 2019.
[301] European Union, 2016, Article 88.
[302] Moeller, C., 2016, p. 157.
[303] Ibidem, p. 158.

as wearables used in the workplace. In conclusion, while the GDPR seems to be a very advanced instrument to discipline the relationship between businesses and consumers in current times, it does not seem to be as good in protecting employees of the Smart Factory, intended both as the Industry 4.0 core and as highly digitalised and automated working environments. Employees are the subjects that need to reaffirm their rights over personal data, thus the new efforts towards the improvement of data protection legislations should be focused on the aforementioned issues.

Conclusion

The aim of this thesis was to analyse the risks arising from the increased production and use of data and the solutions offered by the European data protection framework, with a special focus on the Industry 4.0 environment. This poses very complex challenges with regard to data protection. First of all, in the Smart Factory, which is the fundament of Industry 4.0, machines and humans are deeply interconnected and the management of the supply chain relies to a great extent on data. Secondly, the data produced in such context do not only refer to machines, to production or to industrial processes. Indeed, they can also be personal data, thus causing not only cyber-security challenges, but also informational privacy risks.

However, the data protection framework in Europe has demonstrated its ability to keep pace with the increasing importance of personal data through the years. Not only data protection is recognized as a separate value from privacy, appearing in Article 8 of the Charter; the European Union also outlines specifically the tasks of the Parliament, the Council and the Member States for what regards data protection in the Treaties. All of this resulted in a very recent and advanced instrument: the General Data Protection Regulation.

Nonetheless, the peculiarities of Big Data and new technologies is the speed at which they keep developing and how increasingly they merge in the daily lives of individuals. Therefore, the European data protection framework has to keep evolving too, through increasingly original and innovative instruments. For the Industry 4.0 context, the Directorate of the European Parliament proposed to create a Bill of Rights. Evaluating this proposal is no easy task, because it is not clear what additional protection could such an instrument bring, what characteristics it should have and whether it is necessary or not. What is especially interesting of this proposal is the choice of the instrument, as it conveys the need for a higher law, that disciplines and protect to a deeper level rights that are recognised as fundamental. As it was demonstrated, this case is not isolated: very often the response to new technologies results in the need to exercise fundamental rights and to protect them from the increased threats that are posed to them.

An interesting point that emerged from the analysis is that the GDPR seems to have all the characteristics that the literature described as fundamental for a Bill of Rights. This means that creating a new instrument only aimed at enhancing data protection in general might be superfluous. As a consequence, for what regards the Industry 4.0 context, two

possibilities are outlined: the first one is to create an Industry 4.0 Bill of Rights, that regulates the whole phenomenon and all the rights that might be connected to it. However, the original proposal of the creation of such document was made with specific reference to data protection. Thus, the other possibility, the one that was explored in the third chapter, is that only some elements of the GDPR should be enhanced to make the data processing and exchange in the Smart Factory more protected.

The final finding is that a specific category of subjects is especially threatened in the Smart Factory context: employees. New intrusive technologies are complementing, rather than substituting the human component in the modern production environment. As a consequence, employees produce a quantity of personal data that is not less relevant than the one produced by consumers. The level of protection that is granted for the data of the latter, has to be granted for that of the former too.

In conclusion, a new instrument for the protection of data in the Industry 4.0 context is not strictly necessary. However, it is undeniable that while the GDPR is often focused on the enterprise dimension, many improvements can be made to include to a deeper level the category of employees.

Bibliography

Abrams, Martin. "The Origins of Personal Data and Its Implications for Governance." *SSRN Electronic Journal*, 2014, doi:10.2139/ssrn.2510927.

Accenture. "Redefine Your Company Based on the Company You Keep: Intelligent Enterprise Unleashed." *Accenture Technology Vision 2018*, 2018.

Acquisti, Alessandro. "The Economics of Personal Data and the Economics of Privacy.", 2010, doi:10.1017/CBO9781107590205.005.

AGCOM. *Big Data - Interim Report in the Context of the Joint Inquiry on "Big Data" Launched by the AGCOM Deliberation No. 217/17 / CONS*. 2018.

Arcuri, Maria Cristina, Brogi, Marina and Gandolfi, Gino, "The Effect of Information Security Breaches on Stock Returns: Is the Cyber Crime a Threat to Firms?" *Working Paper*, 2014.

Babiceanu, Radu F., and Remzi Seker. "Big Data and Virtualization for Manufacturing Cyber-Physical Systems: A Survey of the Current Status and Future Outlook." *Computers in Industry*, Vol. 81, 2016, pp. 128-137 doi:10.1016/j.compind.2016.02.004.

Ball, Kirstie. "Workplace Surveillance: An Overview." *Labor History*, 51(1), 2010, pp. 87-106, doi:10.1080/00236561003654776.

Bauer, Dennis, et al. "Movement Towards Service-Orientation and App-Orientation in Manufacturing IT." *Procedia CIRP*, 2017, doi:10.1016/j.procir.2016.06.079.

Ben-Ner, Avner, and Enno Siemsen. "Decentralization and Localization of Production: The Organizational and Economic Consequences of Additive Manufacturing (3D Printing)." California Management Review, vol. 59, no. 2, Feb. 2017, pp. 5–23, doi:10.1177/0008125617695284.

Bennett, Colin J. Convergence Revisited: Toward a Global Policy for the Protection of Personal Data, In P.E. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape*. MIT Press, Cambridge, Ma.,1997, pp. 99-123

Bennett, Colin J. "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?" *Information Polity*, Vol. 23(2) 2018, doi:10.3233/IP-180002.

Bradford, Anu, et al. "The Brussels Effect." *Printed in U.S.A. Northwestern University Law Review*, Vol. 107(1), 2012, pp. 1-67.

Buenaflor, Cherrylyn, and Hee Cheol Kim. “Six Human Factors to Acceptability of Wearable Computers.” *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 8(32), 2013, pp.103-114.

Burrell, Jenna. “How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms.” *Big Data & Society*, Vol.3(1), 2016, pp. 1-12-doi:10.1177/2053951715622512.

Cavoukian, Ann. “The 7 Foundational Principles.” *Identity in the Information Society*, 2010, doi:10.1007/s12394-010-0062-y.

Celeste, Edoardo. “Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology’s Challenges.” *SSRN Electronic Journal*, 2018, doi:10.2139/ssrn.3219905.

Chamorro-Premuzic, Tomas, et al. “New Talent Signals: Shiny New Objects or a Brave New World?” *Industrial and Organizational Psychology*, Vol. 20, 2016, pp.1-20doi:10.1017/iop.2016.6.

Cheng, Long, Fang, Liu and Danfeng Daphne. “Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions.” *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, Vol. 7(5), 2017, doi:10.1002/widm.1211.

Cheng, Mingming, and Carmel Foley. “Algorithmic Management: The Case of Airbnb.” *International Journal of Hospitality Management*, Vol.83, 2019, pp. 33-36doi:10.1016/j.ijhm.2019.04.009.

Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius. The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, vol.28(1), 2019,pp. 65-98.

Clobridge, Abby. “Building a Digital Repository Program with Limited Resources.” *Building a Digital Repository Program with Limited Resources*, 2010, doi:10.1533/9781780630458.

Coase, Ronald H. “The Problem of Social Cost.” *Journal of Law and Economics*, vol. 1(16), 1960, doi:10.1002/9780470752135.ch1.

Cofone, Ignacio. The Dynamic Effect of Information Privacy Law, 18 Minn. J.L. Sci. & Tech. 517, 2017.

Cooper, Tim, and Ryan LaSalle. *Guarding and Growing Personal Data Value*., Accenture Institute for High Performance, 2016.

Davenport, Thomas H. *The AI Advantage: How to Put the Artificial Intelligence Revolution to Work*. MIT Press, 2018.

Davenport, Thomas H., et al. “Competing on Talent Analytics.” *Harvard Business Review*, vol. 88(10), 2010, pp. 52-58.

Davies, Ron. “Industry 4.0. Digitalisation for Productivity and Growth.” *European Parliamentary Research Service*, 2015.

De Minico, Giovanna. “Towards an Internet Bill of Rights.” *Loyola of Los Angeles International and Comparative Law Review*, vol. 37(1), 2015, pp. 1-30 doi:10.2139/ssrn.2681186.

Deloitte. “Realising the Economic Potential of Machine-Generated, Non- Personal Data in the EU.” *2018*.

Deloitte Insights. “Global Human Capital Trends 2018 | Deloitte US.” *Deloitte University Press*, 2018.

“Tech Trends 2019: Beyond the Digital Frontier”. 2019.

Elgesem, Dag. “The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.” *Ethics and Information Technology*, vol. 1, 1999, pp.283-293doi:10.1023/A:1010076422893.

ECtHR 9 December 1994, Lopez Ostra v. Spain, Series A, Vol. 303-C.

European Commission. “A Digital Single Market Strategy for Europe.” *COM(2015) 192 Final*, 2015, doi:10.1017/CBO9781107415324.004.

“Digitising European Industry - Reaping the Full Benefits of a Digital Single Market.” *COM(2016) 180 Final*, 2016.

Digital Transformation Scoreboard. 2018.

“The Digital Economy and Society Index (DESI) | Digital Single Market.” *The Digital Economy and Society Index (DESI)*, 2018.

European Court of Auditors*, Broadband in the EU Member States: Despite Progress, Not All the Europe 2020 Targets Will Be Met*. 2018.

European Union. “GDPR 2016/679 of the European Parliament and the Council of the European Union.” *Official Journal of the European Communities*, 2016, doi:http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf.

Fritzen, Søren, Frédéric Lefort, Oscar Lovera-Perez, and Frank Sänger, *Digital Innovation in Consumer- Goods Manufacturing*, McKinsey Insights 2016.

Gandomi, Amir, and Murtaza Haider. “Beyond the Hype: Big Data Concepts, Methods, and Analytics.” *International Journal of Information Management*, vol. 35(2), 2015, pp. 137-144 doi:10.1016/j.ijinfomgt.2014.10.007.

Gerards, Janneke H. “Fundamental rights and other interests – should it really make a

difference?", in: E. Brems (ed.), *Conflicts between Fundamental Rights*, Antwerp: Intersentia, 2008, at 657.

Gouardéres, Frédéric. "Industry 4.0", Directorate General for Internal Policies - Policy Department A: Economic and Scientific Policy., 2016, doi:10.1007/978-1-4842-2047-4.

Greenleaf, Graham. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108." *International Data Privacy Law*, vol. 68, 77, 2012, doi:10.1093/idpl/ips006.

GTAI. "Smart Manufacturing for the Future." *Industrie 4.0*, 2013, doi:10.1007/978-3-642-36917-9.

Hermann, Mario, Pentek, Tobias and Otto, Boris "Design Principles for Industrie 4.0 Scenarios: A Literature Review." Working Paper, Technische Universität Dortmund, Dortmund., 2016, doi:10.1109/HICSS.2016.488.

Herrmann, Frank. "The Smart Factory and Its Risks." *Systems*, 2018, doi:10.3390/systems6040038.

Heurix, Johannes, and Thomas Neubauer. "Privacy-Preserving Storage and Access of Medical Data through Pseudonymization and Encryption." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011, doi:10.1007/978-3-642-22890-2_16.

Hijmans, Hielke. *The European Union as Guardian of Internet Privacy*. 2016, doi:10.1007/978-3-319-34090-6.

Hoofnagle, Chris Jay, et al. "The European Union General Data Protection Regulation: What It Is and What It Means." *Information and Communications Technology Law*, 2019, doi:10.1080/13600834.2019.1573501.

Information Commissioner's Office. "Big Data, Artificial Intelligence, Machine Learning and Data Protection." *Data Protection Act and General Data Protection Regulation*, 2017.

Institute, Ponemon. "2018 Cost of Data Breach Study, Global Overview." *IBM Security*, 2018.

Jülicher, Tim, and Marc Delisle. *Step into "The Circle"—A Close Look at Wearables and Quantified Self*. 2017, doi:10.1007/978-3-319-62461-7_10.

Kagermann, et al. "Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0." *Final Report of the Industrie 4.0 WG*, 2013.

Kirby, Hon Michael. "The History, Achievement and Future of the 1980 OECD Guidelines on PrivacyI." *Digital Enlightenment Yearbook 2012*, 2012, doi:10.3233/978-1-61499-057-4-83.

King, Madeleine. *Fashion, the body and technology: Tracing early 20th century techno-utopian ideas, aesthetics and impulses in 21st century wearable technology*. Queensland: Queensland University of Technology, 2011.

Klitou, Demetrius. *A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design*. 2014, doi:10.1007/978-3-642-54069-1_6.

Laney, Doug. "3D Data Management: Controlling Data Volume, Velocity, and Variety, Gartner." *Application Delivery Strategies*, 2001.

Lasi, Heiner, et al. "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries April 09, 2015 Michael." *Business and Information Systems Engineering*, 2014, doi:10.1007/s12599-014-0334-4.

Lupton, Deborah. "Understanding the Human Machine [Commentary]." *IEEE Technology and Society Magazine*, 2013, doi:10.1109/MTS.2013.2286431.

Mabkhot, Mohammed, et al. "Requirements of the Smart Factory System: A Survey and Perspective." *Machines*, 2018, doi:10.3390/machines6020023.

Martin, Adam J. "A Textual Analysis of the International Symposium on Wearable Computers: 1997 - 2011 Proceedings." *Proceedings - International Symposium on Wearable Computers, ISWC*, 2012, doi:10.1109/ISWC.2012.31.

Mateescu, Alexandra, and Ahia Nguyen. *Workplace Monitoring & Surveillance*. 2019.

Moeller, Carolin "Are We Prepared for the 4th Industrial Revolution? Data Protection and Data Security Challenges of Industry 4.0 in the EU Context" in Leenes, Ronald, Brakel R. Van, Serge Gutwirth, and de Hert, Paul., *Data Protection and Privacy: The Age of Intelligent Machines*, Hart Publishing, Portland, USA, 2017, pp. 143-166

Montgomery, Kathryn C., et al. "Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection." *Center for Digital Democracy Report*, 2016, doi:10.1016/j.bpobgyn.2010.11.005.

Musiani, Francesca. "The Internet Bill of Rights : A Way to Reconcile Natural Freedoms and Regulatory Needs ?" *America*, 2009, doi:10.2966/scrip.060209.504.

OECD. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2002, doi:10.1787/9789264196391-en.

Page, Tom. "A Forecast of the Adoption of Wearable Technology." *International Journal of Technology Diffusion*, 2015, doi:10.4018/ijtd.2015040102.

Pereira, A. C., and F. Romero. "A Review of the Meanings and the Implications of the Industry 4.0 Concept." *Procedia Manufacturing*, 2017, doi:10.1016/j.promfg.2017.09.032.

PwC. “The Wearable Life 2.0: Connected Living in a Wearable World.” *Consumer Intelligence Series*, 2016, doi:http://dx.doi.org/10.1017/S2042170200007993.

Qi, Qinglin, and Fei Tao. “Digital Twin and Big Data Towards Smart Manufacturing and Industry 4.0: 360 Degree Comparison.” *IEEE Access*, 2018, doi:10.1109/ACCESS.2018.2793265.

Quan-Haase, Annabel, Wellman, Berry, Hyperconnected Net Work: Computer Mediated Community in, 2005.

Redeker, Dennis, et al. “Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights.” *International Communication Gazette*, 2018, doi:10.1177/1748048518757121.

Reeve, April. “Chapter 15 - Master Data Management BT - Managing Data in Motion.” *MK Series on Business Intelligence*, 2013, doi:https://doi.org/10.1016/B978-0-12-397167-8.00015-7.

Reinsel, David, et al. “Data Age 2025: The Digitization of the World From Edge to Core.” *International Data Corporation*, 2018.

Robinson, Neil, et al. “Review of the European Data Protection Directive.” *Rand Europe Technical Report*, 2009.

Rojko, Andreja. “Industry 4.0 Concept: Background and Overview.” *International Journal of Interactive Mobile Technologies (IJIM)*, 2017, doi:10.3991/ijim.v11i5.7072.

Sanchez, Ron, and Joseph T. Mahoney. “Modularity, Flexibility, and Knowledge Management in Product and Organization Design.” *Strategic Management Journal*, 1996, doi:10.1002/smj.4250171107.

Sangeetha, S., and A. K. Sreeja. “‘Big Data a Great Revolution.’” *International Journal of Computer Science and Information Technologies*, 2015.

Segovia Domingo, Ana Isabel, and Nathalie Desmet Villar. *Self-Regulation in Data Protection*. 2018.

Sharon, Tamar. “Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare.” *Philosophy and Technology*, 2017, doi:10.1007/s13347-016-0215-5.

Smith, D. Smart clothes and wearable technology. *Artificial Intelligence & Society*, *3*(22), 2017, pp. 1–3.

Stigler, George J. “An Introduction to Privacy in Economics and Politics.” *The Journal of Legal Studies*, 1980, doi:10.1086/467657.

Tankard, Colin. “What the GDPR Means for Businesses.” *Network Security*, 2016, doi:10.1016/S1353-4858(16)30056-3.

Transparency Market Research. (2013). *Wearable Technology Market - Global Scenario, Trends, Indus- try Analysis, Size, Share And Forecast 2012 – 2018*. Albany: Transparency Market Research

Troiano, Alexandra. "Wearables and Personal Health Data: Putting a Premium on Your Privacy." *Brooklyn Law Review*, 2017.

Van der Lans, Rick. "Data Virtualization for Business Intelligence Systems." *Data Virtualization for Business Intelligence Systems*, 2012, doi:10.1016/C2011-0-07129-6.

Wacks, Raymond. "Privacy : A Very Short Introduction." *Very Short Introductions*, 2010, doi:10.1093/actrade/9780199556533.001.0001.

Wan, Jiafu, et al. "Industrie 4.0: Enabling Technologies." *Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things, ICIT 2015*, 2015, doi:10.1109/ICAIOT.2015.7111555.

Warren, Samuel D., and Brandeis, Louis D.. "The Right to Privacy." Harvard Law Review, vol. 4, no. 5, 1890, pp. 193–220. JSTOR, www.jstor.org/stable/1321160.

Schwab, Klaus. "The Fourth Industrial Revolution". World Economic Forum, Geneva, Switzerland, 2016.

World Economic Forum. *Fourth Industrial Revolution Beacons of Technology and Innovation in Manufacturing*. 2019.

Yusuf, Perwej. "An Experiential Study of the Big Data." *International Transaction of Electrical and Computer Engineers System*, vol. 4, no. 1, 2017, pp. 14–25.

Zeid, Abe, et al. "Interoperability in Smart Manufacturing: Research Challenges." *Machines*, 2019, doi:10.3390/machines7020021.

Zhan, Yuanzhu, et al. "Unlocking the Power of Big Data in New Product Development." *Annals of Operations Research*, 2018, doi:10.1007/s10479-016-2379-x.

Sitography

APEC Privacy Framework, 2005.
https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

Accenture, "Guarding and Growing Personal Data Value", 2016.
https://www.accenture.com/_acnmedia/pdf-4/accenture-guarding-and-growing-personal-data-value-pov-low-res.pdf

Akamai Research," Consumer Attitudes Toward Data Privacy Survey, 2018", 2018
https://www.akamai.com/us/en/multimedia/documents/report/akamai-research-consumer-attitudes-toward-data-privacy.pdf

Bloomerg, "Wearable Technology Market Growing at a CAGR of 15.5% and Expected to Reach $51.6 billion by 2022 ", 2019.
https://www.bloomberg.com/press-releases/2019-07-01/wearable-technology-market-growing-at-a-cagr-of-15-5-and-expected-to-reach-51-6-billion-by-2022-exclusive-report-by

Breach Level Index
https://breachlevelindex.com/data-breach-library

Camera dei deputati, "Dichiarazione dei diritti di Internet", 2017.
https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/note_informative_2017.pdf

CCS Insights, "Wearables Market to Be Worth $25 Billion by 2019", last accessed 07/2019.
https://www.ccsinsight.com/press/company-news/2332-wearables-market-to-be-worth-25-billion-by-2019-reveals-ccs-insight/

CISCO, "Cisco Visual Networking Index: Forecast and Trends", 2019.
https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf

Comparitech, "Analysis: How data breaches affect stock market share prices (2018 update)", 2018,
https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/
.

Council of Europe, "GUIDE TO GOOD PRACTICE IN RESPECT OF DOMESTIC REMEDIES", 2013.
https://www.echr.coe.int/Documents/Pub_coe_domestics_remedies_ENG.pdf

Deloitte, "GDPR in the public sector", last accessed 08/2019.
https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-in-the-public-sector.html

DMA, "DMA insight: consumer privacy- the global view", last accessed 08/2019
https://dma.org.uk/uploads/misc/5b2a5cd7c0268-consumer-privacy--01_5b2a5cd7c01d1.png

EDPS, "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit", 2017.
https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf

EDPS, "Necessity and Proportionality", last accessed 08/2019.
https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

Commission, “Pillars of the Digitising European Industry initiative”, 2018.
https://ec.europa.eu/digital-single-market/en/pillars-digitising-european-industry-initiative

European Commission Press Release, “General Data Protection Regulation shows results, but work needs to continue”, 2019.
https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_19_4449/IP_19_4449_EN.pdf

European Union, “REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018
on a framework for the free flow of non-personal data in the European Union”, 2018.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN
Forbes “A special price just for you”, 2017.
https://www.forbes.com/sites/neilhowe/2017/11/17/a-special-price-just-for-you/#2bffa1c390b3

Forbes “How To Drive Employee Engagement With Workplace Gamification “, 2017.
https://www.forbes.com/sites/danielnewman/2017/11/28/how-to-drive-employee-engagement-with-workplace-gamification/#553fec893cf0

Forbes, “A Fading Twitter Changes Its User Metrics Once Again”, 2019.
https://www.forbes.com/sites/kalevleetaru/2019/04/23/a-fading-twitter-changes-its-user-metrics-once-again/#7a4cf88b7a31

Gartner IT Glossary, “Big Data”.
https://www.gartner.com/it-glossary/big-data

IBM, “Introduction to Big Data classification and architecture”, 2013.
https://developer.ibm.com/articles/bd-archpatterns1/

IDC, “IDC Reports Strong Growth in the Worldwide Wearables Market, Led by Holiday Shipments of Smartwatches, Wrist Bands, and Ear-Worn Devices”, 2019.
https://www.idc.com/getdoc.jsp?containerId=prUS44901819&utm_medium=rss_feed&utm_source=Alert&utm_campaign=rss_syndication

Il Sole24 Ore, “INTERNET BILL OF RIGHTS IN ITALIA”, 2014
https://st.ilsole24ore.com/art/tecnologie/2014-07-20/internet-bill-of-rights-italia-081243.shtml?uuid=ABS0iecB

IOT Insights, “LogMeIn Acquires Pachube”, last accessed 07/2019.
http://www.iotinsights.com/governance/deals-and-finance/logmein-acquires-pachube/

Kagermann, H., Lukas, W., Wahlster, W., “Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution”, 2011.
https://www.ingenieur.de/technik/fachbereiche/produktion/industrie-40-mit-internet-dinge-weg-4-industriellen-revolution/

New York Times, “Introducing the Internet Bill of Rights “, 2018.
https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html

Oreo, “#MyOreo Creation Contest”, last accessed 07/2019
https://mondelez.promo.eprize.com/myoreocreation/

Price Waterhouse Coopers, “Cybersecurity challenges in an interconnected world”, 2015.
https://www.pwc.ru/en/retail-consumer/publications/assets/pwc-global-state-of-information-security-survey-retail-and-consumer.pdf

Proglove, “Mark ONE S”, last accessed 07/2019.
https://www.proglove.com/products/markones/

Proglove, “Mark 2”, last accessed 07/2019
https://www.proglove.com/products/mark2/

Quantified Self.
https://quantifiedself.com

Testbirds,
https://nest.testbirds.com/home/tester .

.Uber, Telematics, last accessed 07/2019.
https://eng.uber.com/telematics/

Xively, last accessed 07/2019
https://xively.com

Summary

In the last decade, some abrupt developments in technology led to believe that an industrial revolution is taking place. This could be compared to the series of industrial revolutions that started in Great Britain in the late 18th century. The difference of the present situation can be found in the fact that the so-called fourth industrial revolution is being planned ex-ante. This is shown especially by the creation of the Industry 4.0 concept, that fuels and represents the fourth industrial revolution. The megatrends behind this recent development can be divided into connectivity, intelligence and automation. The first refers to the fact that all the elements in the factory are made of fully integrated physical and computational components and in turn communicate with one another. Intelligence incorporates all the machines that act intelligently, i.e. what falls under the umbrella of Artificial Intelligence. Automation is the performance of tasks with little or no human support. These three megatrends are what explains the increasing importance and functionality of machines, which can now communicate, calculate, understand and learn, complementing or even substituting humans in the factory.

In this context, Industry 4.0 was born. It was mentioned for the first time in a communication made by Kagermann, Lukas and Wahlster at the 2011 edition of the Hannover Fair[304]. The concept was born as a German project aimed at investing in the national industrial system to make it able to compete at a global level. However, soon it started getting attention from Europe. Its most known definition comes in fact from the 2015 Communication of the European Commission "A Digital Single Market Strategy for Europe"[305] that states:

"Industry 4.0 is a term applied to a group of rapid transformations in the design, manufacture, operation and service of manufacturing systems and products. The 4.0 designation signifies that this is the world's fourth industrial revolution, the successor to three earlier industrial revolutions that caused quantum leaps in productivity and changed the lives of people throughout the world"[306]

Nowadays, Industry 4.0 is known all over Europe and all the Member States have adopted initiatives to implement it. The current state of digitisation of the European industrial

[304] Retrieved from https://www.ingenieur.de/technik/fachbereiche/produktion/industrie-40-mit-internet-dinge-weg-4-industriellen-revolution/ .
[305] European Commission, 2015.
[306] Ibidem, p. 2.

system can be measured by two indexes, the Digital Economy and Society Index[307] (DESI) (Figure 2) and the Digital Transformation Scoreboard (DTS)[308].

The 2018 DESI report shows that all European countries grew in terms of digital performance, led by Scandinavian countries, the Netherlands and the United Kingdom. Those lagging behind are instead Bulgaria, Romania and Greece. The DTS focuses on the results of the European Platform of National Initiatives on Digitising Industry and Industry 4.0-related activities. This index shows that although many initiatives were endorsed by Member States, the great potential of digitisation has not been fully unlocked yet.

A topic of interest in the Industry 4.0 discourse is the identification of its components. No homogeneous literature around the concept seems to exist at the moment. In fact, in the first years of its existence, the literature about Industry 4.0 grew dramatically, leading to a fragmentation in the identification of its features. Some principal elements were identified, i.e. the Smart Factory, the Internet of Things, Cyber-physical Systems (CPS) and Big Data, but to understand what they are and how they interact a literature review will be presented. The first paper analysed is the 2013 final report of the Industrie 4.0 Working Group[309]. From this piece of research, the importance of the Smart Factory emerges right away. The authors do not write about features or elements, as what they really stress in the paper, is the need not to actually consider any aspect of Industry 4.0 as isolated. In the next paper, published in 2014 by Lasi, Kemper and Fettke[310], the authors split the driving forces of the Industry 4.0 phenomenon into application-pulls and technology-pushes, which incorporate many elements. Also in this paper the centrality of the Smart Factory is evident, as many of the other elements identified can be considered as belonging to this subfield. The next paper is "Industrie 4.0: Enabling Technologies" from Wan, Cai and Zhou[311]. They identify two themes of Industry 4.0, that are realizing the Smart Factory and realizing intelligent production and management. Once again the Smart Factory is the core element, followed by CPS and Internet of Things that are its enabling technologies. Finally, in this paper more attention is given to the aspect of Big Data, as the use of CPS in intelligent manufacturing increasingly relies on cheap and

307 European Commission, 2019.
308 European Union, 2018.
309 Kagermann, H., Wahlster, W., Helbig, J., 2013.
310 Lasi, H., Kemper, P., Fettke, H., 2014.
311 Wan, J., Cai, H., Zhou, K., 2015.

secure data. In the paper of Pereira and Romero[312], the Smart Factory is mentioned as a core component specifically. Finally, Vaydia, Ambad and Bhosle focus on Smart Manufacturing, rather than on the Smart Factory, which together with Internet of Things and Industrial Internet of Things form the main drivers of Industry 4.0[313].

From this analysis, it is possible to deduct that there is neither agreement on what the components of Industry 4.0 are, nor on how they interact. However, the Smart Factory is almost always considered a core element, while CPS and the Internet of Things can be defined as technology enablers. Big Data has a fundamental role too, but this became clearer over time. Finally, the definitions of these concepts can be provided, with a special focus on the Smart Factory and Big Data, that are the core of this essay.

CPS are machines that, due to the integration of ICT elements, can perform a variety of tasks autonomously, such as managing industrial operations and process data. When they join together in a network, they form the Internet of Things, that can be defined as when "'things' and 'objects', such as RFID, sensors, actuators, mobile phones, which, through unique addressing schemas, (...) interact with each other and cooperate with their neighboring 'smart' components, to reach common goals"[314].

The Smart Factory was defined by Hermann, Pentek and Otto as "a factory where CPS communicate over the IoT and assist people and machines in the execution of their tasks"[315]. Its main features are modularity, interoperability, decentralization, virtualization, service orientation and responsiveness[316]. Modularity refers to the integration of the elements of the factory, that can be combined in any way to achieve flexibility. Interoperability is the capability of the factory's elements to communicate and cooperate, exchanging information and data. Decentralization is strictly correlated with interoperability, as a more integrated system also entails that components can decide independently. Virtualization refers to the existence of a virtual version of the components of the factory, that allows the simulation and monitoring of its processes. Service-orientation can refer both to the shift from selling products to services that manufacturing industries are witnessing and to the changes in manufacturing IT, that is increasingly divided into services and apps. Finally, responsiveness is the ability to adapt to changes quickly. All these features are also defined as requirements, as the factories

312 Pereira, A. C., Romero, F., 2017.
313 Vaidya, S., Ambad, P., Bhosle, S., 2018.
314 Giusto, Lera, Morabito, & Atzori, 2010, p. V.
315 Hermann, M., Pentek, T., Otto, B., 2015, p. 10.
316 Mabkhot, M., Al-Ahmari, A. Salah, B., Alkhalefah, H., 2018.

which lag behind will struggle to be competitive. However, all these changes also brought some significant challenges. These include standardization, availability of the IT structure, availability of fast internet, non-technological risks and information security[317]. Standardization is fundamental to achieve interoperability and modularity, as it makes the possibility of connecting the elements of the factory easier. To reach this aim, a common architecture for Industry 4.0 would be necessary and different models are being proposed, among them the famous RAMI 4.0. The availability of the IT structure is fundamental, as to reach a high degree of integration the IT structure has to be non-hierarchical too. All these challenges require a fast connection, that allows interconnectedness of the components and protects from the risk of interruptions. Broadband is also an important objective for the European Digital Agenda[318]. The non-technological risks associated with the Smart Factory are complexity, organizational risks and financial risks[319]. The transformation of the factory into an integrated, flexible and automated network leads to increased complexity of the system. This may have negative impacts on the workforce too, that needs to be increasingly skilled. Organizational risks refer in fact mainly to unemployment. Financial risks arise too, because the implementation of the Smart Factory is still very expensive and both national and supranational authorities, as well as companies themselves, have to deal with the funding necessities of the new industrial system. Finally, the last risk of the Smart Factory is information security. It can be divided into safety against disruption of the operations and protection of personal data. The first one refers to the need to ensure that the production process, now almost fully virtualised, is safe from the threats of hacking and sabotage. The protection of personal data is a tricky topic in the Smart Factory, because it is commonly believed that the only informational risks are those related to production, sales and supply-chain related data. On the contrary, the features of the Smart Factory themselves, such as the interdependency of all its elements, entails the production of a great amount of personal data too.

Before getting to personal data it is necessary to analyse this feature of Industry 4.0 on a larger scale. Nowadays it is very common to hear about Big Data, that are defined as

"high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation"[320].

317 Herrman, F., 2018.
318 European Court of Auditors, 2018.
319 Herrman, F., 2018.
320 https://www.gartner.com/it-glossary/big-data

Volume, Velocity and Variety are the features that, by growing dramatically over the last few years, led to the birth of Big Data. Volume refers to the quantity of data that is collected and available, Velocity refers to the speed at which data are created, collected and processed. Variety refers to differences in data formats, structures and semantics[321]. It is important to notice that Big Data belong to the same continuum of Small Data[322], thus companies do not have to deal with something new, but they rather have to gradually adjust to an increasing magnitude.

Greater attention has to be given to the aspect of Variety, which, due to its growth, led to the existence of many types of data. There are eight main lines along which Big Data can be classified: the analysis type, the processing method, frequency, consumers, type, hardware, content, and sources[323]. The analysis type can be real time and batch, which vary according to how fast data can start and finish the analysis process. The processing methods are analytics, predictive analysis, ad-hoc query reporting and miscellaneous and the choice of which method or combination of methods to use is up to each different business. Frequency depends on the availability of the data feed, that is the mechanism that allows the reception of data from their sources. Data consumers are those who actually use the processed data and they can be mainly humans and business processes. Data types can be metadata, transactional data, historical data and masterdata. Metadata are commonly described as data about data (e.g. digital libraries). Transactional data and masterdata both are produced during transactions, but the former can only refer to one transaction. Historical data are usually the record of something that existed or happened in the past. The hardware refers to "the type of hardware on which the big data solution will be implemented"[324]. The content type is the most famous criterion to classify data and it includes structured, unstructured and semi-structured data. Structured data are data that are already or can easily be inserted in a database. Unstructured data are those "data objects whose contents are not organized into arrays of attributes or values"[325]. Finally, the last classification criterion is the data source. Big Data can be machine-generated and human-generated. The generation of data is a very important topic in the Big Data discourse, because much of the uncertainty comes from the fact that it is impossible to

321 Laney, D., 2001, p.2.
322 Jaap, B., Van Doorn, M., Duivestein, S., Van Manen, T., Van Ommeren, E., 2012
323Sangeetha, S., Sreeja, A.K., 2015. However, these criteria were first found in an article published by IBM in 2013. Retrieved from https://developer.ibm.com/articles/bd-archpatterns1/ .
324 Sangeetha, S., Sreeja, A.K., 2015, p. 3270
325 Berman, J.J., 2018, p. 2.

take for granted that machines only generate non-personal data and viceversa. This introduces another classification of data, that is fundamental for this essay, i.e. personal and non-personal data. The latest definition of personal data is the one of the General Data Protection Regulation, according to which "personal data means any information relating to an identified or identifiable natural person ('data subject')"[326]. The definition of non-personal data is not formal and can be deducted simply by exclusion. As anticipated, this distinction became obsolete, mainly because of the changes in technologies and behaviour, that allow people to leave many traces of their activity, preferences and interests. This further explains the uncertainty linked to Big Data. Not only it is difficult to distinguish personal and non-personal data, but often individuals are not fully conscious of providing different types of operators with their personal data. It is possible to identify four different degrees of awareness of data subjects. They can produce provided, observed, derived or inferred data[327]. Provided data are directly produced by individuals, who are therefore fully aware. These data can be produced for example when a user subscribes to a website or a gym. Observed data "is simply what is observed and recorded"[328]. In this case, the individual knows he might be observed by sensors, through cookies etc., but he may not be aware of the actual creation of data pertaining to him. Derived data are new data elements produced in a digital way that pertain to someone just by being derived from other data related to the same individual. He is aware of the creation of the original data, but not of the fact that new information was derived from them. Finally, inferred data are created through statistical and advanced analytical processes, of which the individual is usually not aware.

As briefly introduced earlier, personal data can be found in the Smart Factory too. Identifying personal data in this environment is necessary to understand how current protection tools are being employed or should be improved. First of all, personal data can be a source of advantage, especially through customer innovation, product innovation and market innovation[329]. In fact, data analytics are very useful in customer relationship management and the enhancement of customer experience. Data are used to improve what already exists, but also to unlock the potential of new products and new markets. They are fundamental to understand what consumers really want, resulting in their satisfaction

326 European Union, 2016, Art. 4(1).
327 Abrams, M., 2014.
328 Abrams, M., 2014, p.6.
329 Cooper, T., LaSalle, R., 2016.

and positive economic indicators. However, data are an asset in the Smart Factory and they can generate risks too. They can be divided between those pertaining to the data holder and those about the data subject. The main risk that could damage a company is a data breach, that is defined as "'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."[330] Such events can result from malicious actions but also from the loss of a device or accidental sharing of information by employees and they lead to increased cost for the company. Part of the cost is a lost business factor: customers can "punish" companies that they do not consider trustworthy not only after the breach happens, but also ex-ante, when they are afraid that they will have privacy problems in the future[331].

Regarding data subjects, some risks arise from the repurposing activity, that refers to when data is used for a different purpose from the one for which they were collected. One of the effects of this practice is profiling, which is especially tricky as very often it is actually declared, yet the customer does not fully understand what it may result in. Another consequence of repurposing is the sale of data to a third party. As it was observed before, this can benefit businesses as data in this case acquire a real monetary value. Conversely, for the data subject this can result in further data misuse by the third party. Finally, some risks for the data subject can arise from data breaches. In some cases, the entity that acquires the data will use or misuse them in the same way as the previous holder. In other cases, data breach can lead to identity theft, which refers to when an individual's personal information is stolen and then used in an illegal way.

However, it is possible to be protected against these risks. Some common instruments are de-identification techniques, privacy notices and privacy-by-design[332]. De-identification techniques are mainly anonymization, pseudonymization and encryption[333]. Privacy notices are aimed at ensuring transparency, which is very important as Big Data are intrinsically opaque. To be effective, it has to provide clear information, expressed in clear terms for the customers. Finally, Privacy by Design is the most innovative and comprehensive tool for data protection, as it aims to ensure the pursuit of privacy protection through every phase in the development of a service or a product. Although all

330 European Union, 2016, Art. 4(12).
331 Acquisti, A.,2010, p. 21.
332 Information Commissioner's Office, 2017
333 Ibidem, pp. 73-74.

these tools are very important, the risks arising from the data-driven environment are more complex than the worsening of the customer-enterprise relationship. This is how the need for another protection tool emerges: regulation. By now there is still lack of agreement among scholars on whether data regulation actually benefits the public interest and, if it does, what the right amount of it is. In fact, some scholars of the Chicago school believe that there is a trade-off between data protection and the amount of information available to pursue innovation and other social goals, i.e. a trade-off between privacy and efficiency[334]. The Coase Theorem has been used to prove that data protection generates inefficiencies too. According to this theory, in presence of externalities, private operators can negotiate and internalize them, eventually reaching a better equilibrium of resources[335].

Other scholars believe that privacy can have an absolute value and people can have pure privacy preferences. If this is true, then it cannot be taken for granted that the utility arising from getting the information regarding some individual is bigger than his disutility in losing it and the government has to find the level of privacy that maximizes the production of data, without decreasing the flow of information. Although the dilemma of the necessity of data protection is unsolved, this instrument is very important in Europe, that became the "leading paradigm in information privacy"[336]. As a consequence, it is vital to analyse the history and development of data regulation.

It is necessary to begin with the modern concept of privacy, which originated in the United States and traces back to the end of the 19th century, when two lawyers, Samuel Warren and Louis Brandeis, defined it as "the right to be let alone"[337]. This right gained international recognition right away, as in 1950 it was introduced in Article 8 of the European Charter of Fundamental Rights. However, soon the concept of data protection started emerging as an individual value, creating a new dilemma on the scope of the rights to privacy. Some scholars believe that, once demonstrated that individual interests can be protected with the instrument of the European Convention, most of the interests related to data protection fall under the same protection of the right to privacy, i.e. the two rights overlap[338]. According to other scholars, the right to privacy limits power, while data protection catalyses power. Thus, the two rights are separate and supplement each other.

334 Cofone, I., 2017, p. 521.
335 Coase, R.H., 1960.
336 Cofone, I., 2017, p. 521.
337 Warren, S.D., Brandeis L.D., 1890.
338 Hijmans, H., 2016..

The European regulatory framework seemed to support this solution as now both rights exist as fundamental rights that are part of one system[339].

Before going into detail of the European regulation, it is necessary to mention the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"[340] of 1980. Although these guidelines were non-binding, they had great influence on the creation of European and national legislations. Eight principles were identified by the responsible committee: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. The importance of these principles is that they are technologically neutral and not limited to any industry or sector and they are written in a simple way, perfect for the complexity of the topic.

The next landmark is the Council of Europe Convention 108, the first European binding instrument that focuses exclusively on data protection. The principal aspect of this document is that it has some principles that are directly found in the OECD Guidelines, while other that are fully European. This distinction makes the reader understand how important the influence of the OECD was and, at the same time, how much European principles will influence non-European legislation[341].

The Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data constitutes the first appearance of the right to data protection in European secondary law. This document was promulgated in 1995 and it is the consequence of the increased use of data in many industries and applications. In this document the influence of the OECD is still evident, however there are two main advances: the centrality of data processing and of data flow[342]. This shows that Europe was aware of the necessity of a deeper level of protection, not only because the use of data was changing (the Directive is the first document that acknowledges further processing), but also because this would have promoted harmonisation of regulation in Europe, making the flow of data in the internal market smoother.

As the Directive 95/46 represented the main appearance of data protection in secondary law, it is necessary to mention how data protection is included in European primary law.

339 Data Protection was introduced in Article 8 of the Charter as a separate right from that of privacy.
340 OECD, 1980.
341 Greenleaf, G., 2012.
342 Elgesem, D., 1999.

Article 16 of the Treaty on the Functioning of European Union is the legal basis of the European data protection framework and its main role is to lay down the mandate of the European Union for what regards the right and data protection and to discipline the relationship between European Union and its Member States in this regard[343]. In particular, the European Court of Justice has to guarantee the respect of Article 8 of the European Charter of Human Rights. The European Parliament and the Council have to implement data protection legislations. Finally, independent authorities have to be vested by the Union with the power to enforce and control the respect of data protection rules. From Article 16 TFEU it also emerges that the competence of data protection is shared with the Member States.

Although one of the aims of the Directive was to reach a certain degree of harmonisation, there were still many differences between countries. Moreover, technologies kept developing, making the Directive obsolete. This is why in 2012 the draft of a new regulation was proposed. The final proposal was made by the Council in 2015 and the agreement with the European Parliament was reached in 2016. The General Data Protection Regulation was finally enforced in May 2018. With this new set of rules the definition of personal data was widened, including every information that could lead to the identification of an individual. In general, the rights of data subjects are increased and the obligations of data holders too. However, the real innovative reach of the GDPR can be found in another aspect, which will be analysed later on.

Going back to the core of this essay, i.e. the Smart Factory, it seems natural to wonder whether this legislative framework ensures sufficient protection against the risk that arise from the use of personal data in the Industry 4.0 context. A very interest document was published in 2016 by the Economic and Scientific Policy Department of the Directorate for Internal Policies of the European Parliament[344]. Although in 2016 the GDPR was already reality, this paper sheds light on the possibility of creating a different kind of tool for the protection of data: A Bill of Rights of Industry 4.0. According to the authors, individuals need to reaffirm their rights over data, thus needing such a new legislative instrument. Assessing this proposal is the aim of the following pages. To do so it is necessary to understand why such a suggestion was made in the first place, why it was suddenly abandoned and if the enforcement of the GDPR influenced the development of this idea. The starting point proposed in the Directorate's document is the Smart Glove

343 Hijmans, H., 2016.
344 Gouardéres, F., 2016.

case study. The Smart Glove was invented by a start-up called ProGlove in 2014. It acquired success right away and nowadays it is used in all the plants of BMW and most of the European automotive firms. The Smart Glove is made of two components. The first one is the wearable glove and the second is a computational core. The result is a device that can be worn by workers and help them performing many types of tasks (mainly Picking, Assembly, Packing and Staging). Of course, this tool relies on data a lot: it can scan barcodes, sense weight and heat, provide the worker with real-time feedback during the performance of a task and much more. Once again, one may think that the only risk arising from these data is industrial espionage or in general, cybercrimes. However, the Smart Glove produces also many personal data, such as the location of the worker, his habits and the way he performs the tasks[345]. Although this case may seem an ordinary situation in which personal data are collected and stored in an ambiguous way, there are some peculiarities that inspired the Directorate to believe that the personal data used in Industry 4.0 need further protection. One reason might be the fact that this specific tool is both created and used in this environment. Another interesting aspect could be related to how blurry the line between physical and computational spheres becomes with tools such as the glove, i.e. the so-called wearables. A wearable is defined "as a material product, specifically a garment or accessory worn on the body that is inspired by, created through, or enhanced by digital or electronic technologies"[346]. The market of such devices reached huge dimensions and it is set to reach a value of $51 billion by 2022. This poses unprecedented issues for data protection. Although it was shown that the GDPR kept adapting to increasingly advanced technology, from the augmented presence of the internet to the spread of mobile devices and how they fully merged with the daily life of people, this might not be enough. The difference of wearables, is that they do not only represent the merging of mobile devices with daily lives, but with individuals, their clothes, their bodies and their health. The result of this is the creation of a new identity, the quantified self, and of a wide set of personal and sensitive data. The quantified self could be defined as the result of the habit of tracking physical, health and body-related data and analysing it in order to optimise one's behaviour. This entity is extremely controversial as the benefits and risks arising from the collection of such data are in deep contrast and produce not only legal but social implications[347]. One dichotomy that

345 Retrieved from https://www.proglove.com/
346 King, M., 2011, p. 8.
347 Sharon, T., 2017.

characterises the quantified self is that between empowerment and surveillance. On one hand the individual is called to action and feels like has more control over himself. On the other hand, he makes the possibility of surveillance something which is not given from above anymore. Another dichotomy is that between the trustworthiness of numbers and the risk of reductionism. Numbers allow individuals to have a high degree of personalization in the services they receive and of comprehension of themselves, their activities and behaviours. However, often an excessive trust in data and quantification can lead to a distorted and incomplete view of reality, because the algorithms and data use symbols and indicators that only approximate the real values that are being measured. Although these devices are very controversial, what matters for this essay is that their users willingly provide some operators with a whole set of sensitive data, that are going to be used in a way they do not fully understand. The next question seems natural. To believe that individuals need to be further protected means that the regulation currently in place, the GDPR, is not sufficient. In reality the GDPR shows real progress in ensuring protection against many of the risks that could be caused by wearable devices[348]. For example, most of the data produced belong to the category of sensitive data, the processing of which is generally prohibited. This has an impact on processing automated decisions that should not be based on sensitive data, unless the special requirements for the processing of such data are met and special safeguards are in place too. Special categories of data are also additionally protected when processed on a large scale, as data protection impact assessments become mandatory in such circumstances. However, the GDPR shows some flaws too. One of them is the set of derogations to the prohibition of processing special categories of data, that seems to be expanded, even in the case of health-related data. Finally, other problems arise with the derogations relative to public interest matters. Both the further processing of data prohibition and the data storage limitations are derogated when it is justified by scientific, historical and research purposes.

Once it is admitted that the GDPR might not be sufficient, it is necessary to analyse the solution proposed by the directorate: the Bill of Rights. This proposal is inspired by many discussions, that are still in place, around the possibility to create an Internet of Things Bill of Rights. To understand how such tool would be different from traditional regulation, some of the literature about Bills of Rights and IoT Bills of Rights will be

348 Montgomery, K., Chester, J., Kopp, K., 2016.

used. This is possible because a new phenomenon is developing: digital constitutionalism. The circumstances in which people feel the need to exercise their fundamental rights have increased, due to the new threats posed by digital technologies. As a consequence, the constitutional ecosystem is reacting to this changed environment by creating a set of principles and rules that lead the response to these new challenges. Regarding the principles, according to Alston, a Bill of Rights should have three main characteristics: 1) The protection of significant rights; 2) The ability to be binding for the government; 3) Redress, in case of right violations[349]. The first one refers to the fact that Bills of Rights were born as declarations aimed at protecting fundamental rights and human liberties. Of course, this is a big source of complexity, not only because the existence of fundamental rights and their value through time cannot be explained, but also recognizing a right is especially difficult due to differences between nations, cultures and social realities. The second characteristic can be explained by the fact that a Charter of Rights is somehow a higher law, to which other lawmakers have to adjust. Finally, redress is a powerful instrument necessary for their respect and as such it has to be granted. Apart from these characteristics, that are strictly necessary, some other features were outlined. First of all, the authority to be entitled with the task to create such an instrument should be a supranational body. Secondly, an equilibrium should be found between regulation and self-regulation. The legislator should be an architect, that is in constant communication with private parties and that does not try to define individual behaviour, rather than a general structure and that will intervene in case of deviations from this structure[350]. Finally, the last features pertain to the content and to the way the lawmaker's powers can be limited, which is fundamental when basic rights are at stake. They are necessity, proportionality and indispensability, which will be explained later on[351].

As mentioned earlier, the Directorate's document was written and published in 2016, the year in which the European Parliament and Council agreed on the text of the GDPR. Thus, it is natural to wonder whether the GDPR is the type of tool the authors were wishing for when writing the document. To answer this question, it will be necessary to see if the features that define a Bill of Rights can be found in the GDPR. Firstly, data protection is recognized by the European Union as a fundamental right as in Article 8(1) of the Charter of Fundamental Rights of European Union and Article 16(1) of the Treaty

349 Klug, F., 2007.
350 De Minico, G., 2015.
351 Ibidem.

on the Functioning of the European Union. Thus, the GDPR respects the first principle of Alston. The GDPR is also binding for the executive. Public authorities have to comply with it and in particular for them it is mandatory to employ a Data Protection Officer. Moreover, for them the legitimate interest is not a sufficient ground for data processing anymore. Finally, the right to redress requirement is met too, as the individuals whose data have been violated can file a complaint with their national DPA and they can act autonomously against the violator. When they are not satisfied with the job of the DPA, they can act against it too. The GDPR also has the other features that were earlier identified.

This tool constitutes a good example of co-regulation, as it has a mixture of a basic legislative act and voluntary agreements between the parties concerned aimed at respecting the legislative act[352]. Finally, the criteria of necessity, indispensability and proportionality are met too. The right to data protection granted by the GDPR is only limited when it is necessary for protecting other rights and freedoms and when the advantages resulting from the limitation of the right do not outweigh the disadvantages of its exercise. This was proved by the EDPS opinion 3/2016 on the European Criminal Records Information System's proposal to facilitate the exchange of information of third-country nationals with the aim of fighting against crime and terrorism. In fact, the use of biometric data to ensure the identification of criminals was deemed as unnecessary as other means could serve this purpose. Conversely, accessing the convictions of third-country nationals was considered a proportionate measure to protect individuals. As it was proved in the previous lines, the GDPR seems to have all the requirements to be defined a Bill of Rights. However, some observations seem necessary. The first requirement of a Bill of Rights according to Alston, is that it has to protect fundamental rights. It is obvious that the scope of the GDPR only includes one fundamental right, i.e. data protection, which means that it can be identified as a Bill of Rights of data protection, but surely not as an Industry 4.0 Bill of Rights. Such an instrument would have to be created from scratch, possibly respecting the requirements mentioned in the previous paragraphs and understanding whether it is necessary or not. The question whether Industry 4.0 needs to be regulated per se would have to be answered. Conversely, the Directorate's document states that a Bill of Rights is specifically necessary to *control data* in the Industry 4.0 context. If this is the right interpretation, what the authors were

352 European Union, 2011.

wishing for is a Data Protection Bill of Rights that increases protection in the Industry 4.0 context. Although an Industry 4.0 Bill of Rights per se is not necessary, this does neither mean that sufficient tools for the protection of data in such context are already in place, nor that the GDPR cannot be improved in that direction. Finally, one suggestion might be to improve the protection of personal data produced by employees. The very essence of the Smart Factory entails that remote working is increasingly implemented as, thanks to CPS, very often workers do not need to get physically in contact or even close to the machines they use or produce. This and the spread of wearables devices in the workplace are dramatically increasing the degree of intrusiveness of surveillance. Although the worker expects to be controlled, it is difficult to establish when it becomes too much. Some practices can generate very bad downturns[353]. Modern technologies are able to flag performance and behaviours of employees, as well as their emotions. Some common tools are dedicated to remote monitoring, by tracking the time that an employee spends on the computer and even keystrokes. Although this might result in increased efficiency and productivity, it also puts the worker under an unprecedented pressure. This happens also because many of these technologies use the mechanism of gamification, that drives individuals to perform and strive for better results, in exchange for immediate gratification[354]. Furthermore, part of the competition is also based on physical performance as often health related data are collected too, thanks to wearable devices. The GDPR considers the category of employees, contrary to the Directive. However, it states that Member States should "provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context"[355]. This is a step back relative to the harmonisation efforts that took place in the past years, because leaving space to Member States to act individually means that not all the countries will take action and the resulting legislations will constitute a very diverse framework, undermining efficiency for European international companies[356]. In conclusion, the GDPR seems to be a very advanced instrument to discipline the relationship between businesses and consumers, but not to protect employees of the Smart Factory. Finally, the efforts towards the improvement of data protection legislations should be focused on the aforementioned issues.

353 Mateescu, A., Nguyen, A., 2019.
354 See https://www.forbes.com/sites/danielnewman/2017/11/28/how-to-drive-employee-engagement-with-workplace-gamification/#553fec893cf0
355 European Union, 2016, Article 88.
356 Moeller, C., 2016, p. 157.