Università
Ca'Foscari
Venezia

*Master's Degree*

*in Data Analytics*

*for Business and Society*

*Final Thesis*

# Protection of Workers' Personal Data in the Context of Industry 4.0

**Supervisor:**
Prof. Alessandro Bernes

**Graduand:**
Anna Sanchini
Matriculation Number
874959

**Academic Year**
2022/2023

# TABLE OF CONTENTS

## ABSTRACT

For many years, we have been witnessing a process of a drastic transformation due to the development of new ICT that, while revolutionising positively many sectors of our society, strengthening and improving almost all activities, on the other hand, they have also enhanced many challenges and insecurities, especially in the employment context in such a way that attention to privacy and data protection has been growing with an increased pace and relevance. In the last decades, besides the concept of "privacy", it has introduced the concept of "Data Protection", differs from the previous concept since it refers to ensuring the proper use of personal data by giving individuals control over how their data is accessed, used or shared. Today the General Data Protection Regulation (GDPR, 2016/679/EU) has provided a harmonised, consistent, and comprehensive framework for the processing of personal data.

In the employment context, however, the GDPR has enacted only Article 88 which explicitly focuses on the workers' data protection, leaving to the Member States the obligation to amend or replace their respective national data protection laws to align with the GDPR. Regardless of the great importance of individual rights in the employment context, the European Union has not already established harmonised rules.

The first chapter deals with the topic of Industry 4.0, the starting point of digital transformation, its principles and the associated technologies, with a focal point on the evolution of the employment context.

The second chapter focuses on the evolution of workers' personal data protection during history and underlies the issues that the GDPR has brought.

Lastly, the third chapter focuses on the remote control of workers. Thus, it will be analysed as the reform of Article 4 of the Workers' Statute, since it came at a time when it was no longer possible to ignore the impact of technological innovation on labour relationships, has evolved after the Jobs Act, and it will be pointed out which are the conditions for the lawfulness of the use of personal data obtained through remote control.

# INTRODUCTION

In contemporary times, the use of new technologies is becoming more and more frequent, to the point of inducing us to evoke the concepts of "technological society" or "digital society" to describe the economic, social and productive context in which we operate and live today.

The use of technological innovations in today's reality also explains several purposes, because of their intrinsic flexibility and adaptability, which lend themselves, in a transversal perspective, to be applied to multiple and heterogeneous disciplines, as well as to public and private areas indiscriminately and not only with purely relational purposes but also productive. Within companies, if the use of technologies and automated equipment sometimes arises as a necessity closely related to the activity rendered, in other cases, instead, is the tool through which to achieve the objectives divided with lower use of resources or in a shorter time or, even, with greater final effectiveness, in a general efficiency of the production process. In these last cases, therefore, the use of the technologies is not placed in a relationship of narrow necessity, but of business convenience.

On the individual level, the pervasiveness of new technologies in everyday life is now evident, as are the reflections that the massive use of computer equipment has produced in all fields of human action, which over time has undergone a progressive metamorphosis of its traditional features. We are living in an era in which "technology has become pervasive like the air we breathe"[1] since the IT-technological innovations have radically changed not only the relational and social dynamics, making accessible the weaving of communications even at a considerable distance, but also the political, educational, health and, finally, economic production and the labour market.

Technological evolution has therefore shaped and reshaped different areas of our individual life, both personal and working, but also collective and social, accelerating the pace of introducing change and innovation. Such circumstances are witnessed not only by the ease with which the new generations (the digital native) approach the use of electronic devices but

[1] A. Khanna, P. Khanna, *L'età ibrida, il potere della tecnologia nella competizione globale*, Codice Edizioni, Turin, 2013.

also by the massive use of cameras, which, twenty years ago began only to spread, today not only dot public and private spaces, becoming a familiar presence but are also able to perform more complex functions, such as the recognition of persons, the classification of their behaviour or the tracking location while they are working.

However, the boundaries between the autonomous and conscious projection of the individual in the virtual space and its private dimension are becoming increasingly blurred, imposing a revision of the same notion of privacy known until now.

If originally this concept, evoking the scheme of private property, implied the need to exclude others from their sphere understood as confidential, now the notion has changed, acquiring a more dynamic and extensive sense, such as to include both the right to follow the path that your personal information focus and the right to oppose the misuse of the same. This conceptual difference can also be easily grasped at the supranational level and in the Charter of Fundamental Rights of the European Union. In the latter, the right «to respect for one's private life», enshrined in art. 7, which implies static and negative protection, is kept separate from the right «to the protection of personal data» referred to in art. 8, the protection of which results in a set of rules on how data are processed and circulated.

It becomes increasingly important to delineate the characters, if not the outlines, between the technology of freedom and the technology of control.

In this context, to avoid being subjected to sneaky forms of "technological slavery", to which we risk resigning in exchange for apparent utility and digital services, the construction of a system of safeguards of the right to the protection of personal data, which is the only way through which to elevate the person and bring it back to the centre of a technological development, which otherwise turns out to be dystopian. Technological development, as well as being technically possible, must be legally and ethically lawful and legally and socially sustainable. Protecting the right to privacy and the protection of personal data, especially where referred to the worker's person, means "combining technology and humanity, freedom and security, public transparency and privacy, information and dignity, economic initiative and individual autonomy, science and freedom from determinism"[2].

[2] A. Soro, *Persona, Diritti, Innovazione. Discorso del Presidente* - Report of the year 2016, Guarantor of the protection of personal data. Cfr. the entire report presented by the Garante on 6 June 2017 at the Sala della Regina in Palazzo Montecitorio.

The above-mentioned requirements, aimed at regulating new forms of protection of the fundamental values of the human person, to ensure that they are up-to-date and not obsolete compared to the new control tools of the children of the digital age, they emerge more strongly in the labour market, both in the genetic phase of the relationship and in the purely executive phase. The greatest delicacy that characterizes the working environment derives from the values that intrinsically underlie it, constituting not only the tool through which the worker draws his income and his source of sustenance, but also the place and the occasion in which it rises and carries out its personality by art. 2 Cost., thus emerging the centrality of the dignity of the worker.

This research, therefore, aims to investigate whether and how the increasingly frequent introduction of computer tools and algorithmic logic within the company has affected the relationship between the power of employer control, now predominantly technological, and the requests for privacy and confidentiality claimed by workers even within their professional sphere.

It is therefore the intention of the thesis to verify whether technological progress has contributed to the emancipation of the employee or in any case to the pursuit of greater business efficiency without any detriment to the position of the worker or if, on the other hand, has irremediably determined the employee's exposure to the employer's electronic eye, able to capture every aspect of his professional and private life.

The underlying rationale for dealing with these new issues and the analysis set out below must, however, be seen in the necessary awareness that although technological innovations have changed society and the relationships that develop within it, it is still society itself, as a political actor, to determine how computer equipment-technology and the use of the data collected therein.

Therefore, it is society that has the power and at the same time the duty to use new technologies in an environment where fundamental rights and freedoms, albeit re-read in the light of new criteria compared to the past, are still guaranteed, to avoid technological progress resulting in a regression of the protections of the constitutionalized person, having on the contrary to hope for the construction of a sustainable innovation.

# CHAPTER 1 – The Impact of Industry 4.0 on Employment Relationship

## 1.1. Introduction to Digital Transformation

In recent years, our society has been affected by many disruptive technological changes, which have drastically changed many aspects of people's lives: from the economic, social, and cultural aspects to the workplace environment. The epoch of technological changes has been characterised by four important revolutions, which are essential to analyse to comprehend the overall process of technological revolution, and thus, to understand how we have reached the avant-garde of our days. Essential is to consider the term "revolution" as all those disruptive changes that had huge impacts on our society and economy.

The first industrial revolution began at the end of the 18th century, with the development of steam engines and waterpower in manufacturing. It was the first time that technological innovations were applied in the context of industrial purposes, and this led to an overall increase in the context productivity of food and wool.

Moving to the beginning of the 20th century, the second industrial revolution developed through the discovery of two main elements: mass production and electricity. This revolution has brought an important shift that goes from steam engines to machines powered by electricity. Henry Ford was the pioneer of the "assembly line production" which allowed the production of goods to be pulled down the line and built-in partial steps. This new method has positively impacted the production world, by drastically reducing costs and time consumed.

Later, starting in the 1970s, the third industrial revolution was triggered by partial automation using computers, information, and communication technologies. This innovation gave humans the great opportunity to automate an entire production process without the need for any human assistance, given the invention of the first programmable logic control system in 1969. The aim of Industry 3.0 was to increase flexibility, cut the production cycles, customise products for consumers, increase the accuracy of the process and be faster to change when demand changes.

The most recent industrial revolution is instead the fourth one, denoted as Industry 4.0. This last revolution has kept the big advantages already introduced by the previous revolutions, but, moreover, it has implemented technological innovations directly inside the business

processes to improve the value chain during the product life cycle. The terminology “Industry 4.0” is often denominated as “the Internet of Things", “the Internet of everything”, “the cyber-physical system”, “smart industry”, and many other terms and concepts that have in common the willingness to transform traditional manufacturing and production with more digital and sophisticated techniques.

From a historical point of view, the term “Industry 4.0” arose in 2011 during the Hannover Fair when the project “Zukunftsprojekt" was introduced. The project was born to innovate the German production system to lead worldwide. Since other countries were also sharing the same idea based on the belief that digitalization in the manufacturing sector was needed to compete in the market, this revolution has kept, as the main objective, the willingness to digitise any aspect that surrounds humans: starting from industrial machines to reach the automation of any daily human activity, combining the physical world with the virtual one, to design a completely digital environment.

Finally, the main objective of each of the four industrial revolutions was to increase productivity, and in fact, there has been an enormous shift in the production field from the first revolution to the last, passing from steam engine machines to processes almost completely digitised and automated. In the image below we can observe a summary of all the steps of the Industrial Revolution.

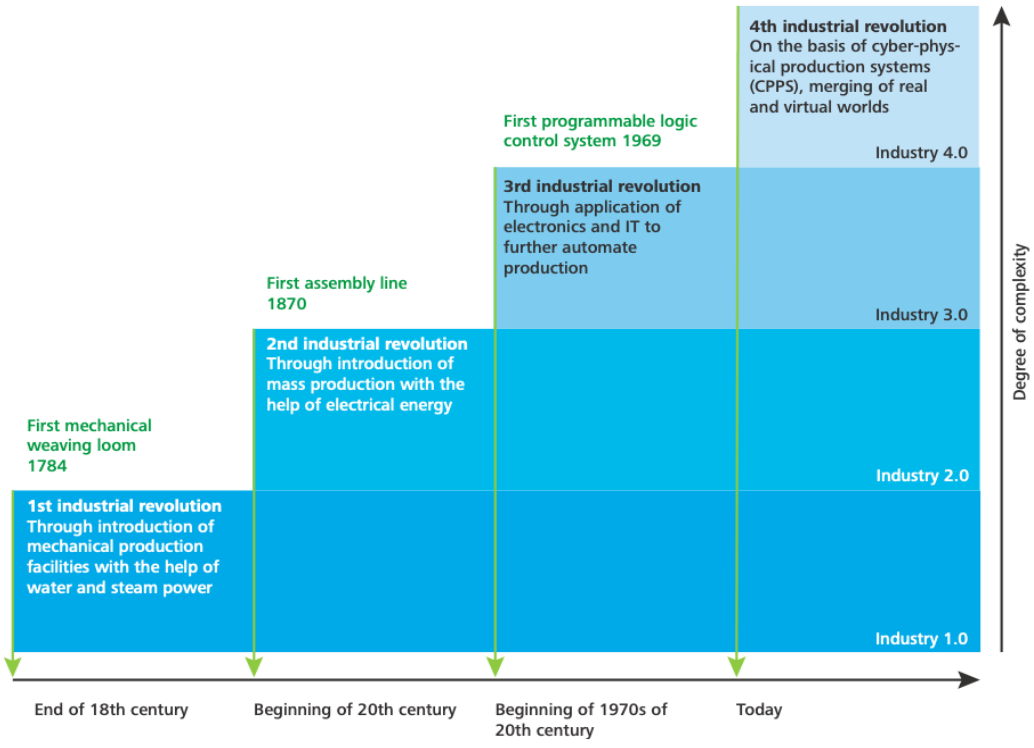


Figure 1.1: Font: Industrial Revolution phases (Source: Schlick et al., 2012)

## 1.2. The New Digital Era: Industry 4.0

Industry 4.0 refers to a new organisational approach that focuses on the interconnection and collaboration of resources to increase production efficiency, productivity, and diversity and decrease all related barriers. In other words, the fourth industrial revolution consists of the virtual union of new production technologies and innovative changes, also named "enabling technologies" since they are inventions that lead to radical changes[3]. There have been many discussions concerning the terminology used for identifying this new paradigm, according to one of the most relevant business consultants, Deloitte[4], the four main characteristics are the following:

- Vertical networking: the intelligent production process creates a cyber-physical space thanks to which the production system can instantly react to any changes and therefore adapt and stay competitive in the market. Industry 4.0 can generate an enormous quantity of data, which after being studied and analysed can be exploited to get new insights, support decision-making and, most importantly, create competitive advantages.
- Horizontal Integration: predicts the creation of networks along the entire value chain. The main objective from a company's point of view is to create cooperation with its suppliers, subcontractors, and customers, to obtain important advantages in terms of optimization of production, possibility of implementations of changes in real-time, reduction of the margin error and increase flexibility.
- Through-engineering: a new approach that enables us to consider all the changes related to a product's lifecycle and during the entire value chain process. The best potential for innovations lies in the organisation of a company, how it is structured, its processes, networks, business models, and its relations with customers. This new method allows us to collect a lot of data.

[3] G. Culot, G. Nassimbeni, G. Orzes, M. Sartor, *Behind the definition of Industry 4.0: Analysis and open questions*, International Journal of Production Economics, Elsevier, Amsterdam, vol. 226(C), August 2020.
[4] Deloitte, *Industry 4.0. Challenges and solutions for the digital transformation and use of exponential technologies,* Zurich, 2015, PDF.

- which is very useful for life cycle management. Moreover, by analysing data and processing them they can generate great indicators for companies to better meet the needs of their consumers and so be able to customise the product.

- Exponential technology: which has been the main driver of the fourth industrial revolution. With the term "exponential" we refer to all those tools able to double in capacity and performance, such as computers, 3D printing, drones, robotics and artificial intelligence. If in the past these tools were affordable only by the military for example, nowadays the price-performance makes it possible to be used by many other parties for daily business activities.

So, when considering the term Industry 4.0, we commonly identify the technological transformation that is affecting all domains of the economy: production, consumption, transport and communications. New technologies and digitalisation represent not only a change in the labour market but a real revolution. It is guided by the interweaving of digitization, which is based on the introduction of devices and processes capable of transmitting and processing huge masses of data with a speed previously unthinkable, and automation, which is the availability of machines capable of performing tasks of medium-high complexity, hitherto the prerogative of human beings alone. The human component, however, is not to be considered superfluous, with a consequent decrease in the places of work. We will see how workers will always be present, but with different tasks such as support, control, and organisation, in general, less repetitive and safer[5].

Two fundamental aspects to consider when it comes to Industry 4.0 are security and privacy. Data security and privacy protection are essential to ensure that the data collected is used responsibly. Available to companies are many security systems used to protect sensitive data from unauthorised access and to ensure that data is processed in the privacy of customers. It is up to companies to engage in informing themselves and investing properly in their security and customers.

Industry 4.0 is therefore the application of all those advanced digital technologies to improve production and efficiency in the industry. Connectivity, automation, artificial intelligence and data analytics, flexibility and security are some of the most important aspects to consider when talking about Industry 4.0.

[5] Report McKinsey Global Institute, *Automazione: come cambia il lavoro? Quale impatto su crescita e produttività,* January, 2017.

### 1.2.1. Enabling Technologies

The evolution of the world of work has always been characterised by having involved, in its main stages, disruptive impacts suitable to reflect on the entire socio-economic reality of the moment. From a diachronic point of view, it is possible to draw an evolutionary line that from a system mainly, if not exclusively, based on the physical strength of man and an agricultural-artisanal system, has shifted more and more towards an industrial system, where the use of machines has taken a central place, until reaching the most recent stages, characterised mainly using digital technologies. The machines, from the preponderant role assumed with the industrial revolution, have gradually separated their dependence on the human factor, up to almost reversing the original relationship.

The possibility of transforming the entire industry with the fourth industrial revolution has been possible because of the great combination between the internet and digital technologies with the physical world, this union leads to the birth of intelligent realities interconnected with each other. The new technological innovations have a leading role in the digital world in which any human is connected.

According to the European Commission, enabling technologies are those technologies with high knowledge intensity and associated with high R&D intensity, rapid innovation cycles, substantial investment expenditure, and highly skilled jobs[6]. Moreover, they have a fundamental role because they contribute to giving higher quality to the production value-chain, by enhancing innovation not only in processes but also in the final products and services.

To understand the overall structure of the fourth industrial revolution, it is interesting to mention the nine enabling technologies applying to industry 4.0: Big Data Analytics, Autonomous and Robotics systems, Simulation, System Integration, the industrial Internet of Things, Additive manufacturing, Augmented reality, Cloud Computing and Cybersecurity. Throughout our analysis, we will just focus on those enabling technologies that are more related to our central topic, which is the analysis of how the employment environment has changed followed by the changes in the context of personal data processing, after Industry 4.0.

[6] Pwc EU services on behalf of the European Commission, *Boosting the Potential of Key Enabling, Belgium*, in: https://www.cecimo.eu/wp-content/uploads/2016/03/KETs-skills-brochure_with_CECIMO.pdf, 2016.

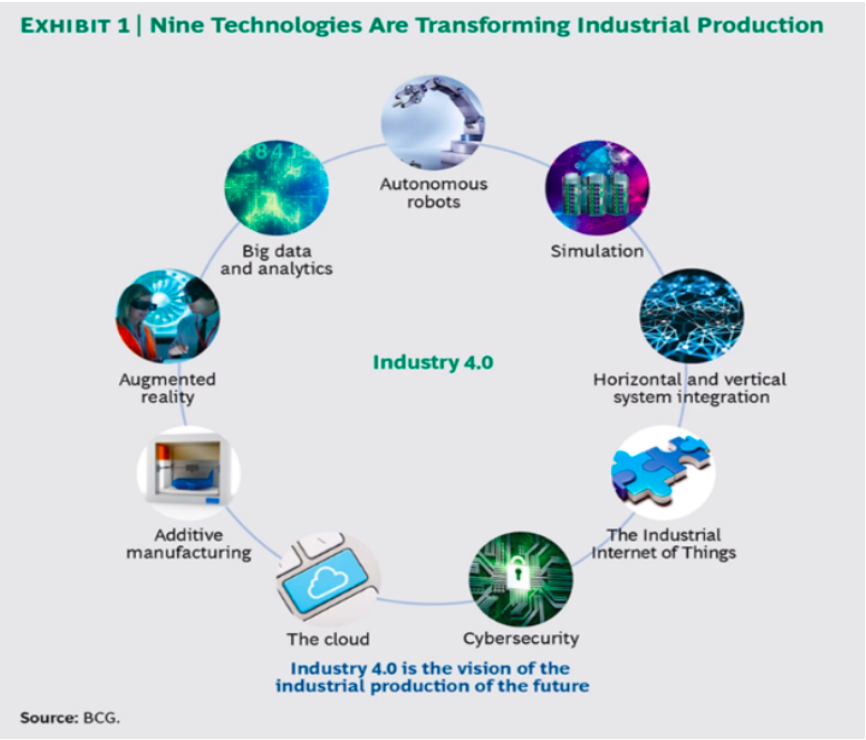


Figure 1.2: Font: Industry 4.0: the future of productivity and growth in manufacturing industries.

*Big Data Analytics* is what distinguishes the fourth industrial revolution since it is mainly centred on the collection of data and information of any kind, collected at any time. Obtaining and using data represents the biggest challenge for analysts and managers who support decisions not only in the long term but also in the short term, thanks to their continuous availability.

The name "Big Data" has been attributed precisely to the huge quantity of data that nowadays institutions have available and for their diversity; they derive from new sources that are added to the traditional ones managed by internal databases of the enterprise. Data, once collected and analysed, can be converted into knowledge since data can be used to identify trends and patterns between inputs, processes, and outputs, and this allows companies to improve many aspects or processes of their use. The collection of huge amounts of data can create many opportunities and advantages for companies but can also create dangerous situations if processed by parties not authorised.

Around the scenario just outlined, parallel to the growing enthusiasm of public and private operators, there was a lively legal reflection. Scholars of privacy law, competition, insurance, finance, and labour relations are confronted, with an increasing frequency, with the potential

of big data analytics[7], sometimes outlining critical scenarios about the guarantee of fundamental human rights. At the heart of the investigation of labour law is the impact of this information on the management of the individual employment relationship.

On one hand, it is pointed out that "sample analysis, combined with big data, can reveal detailed information on each worker (in particular on performance cycles)"[8] and at the same time provide useful elements for recruitment, human resource management and other internal activities. On the other hand, and similarly to what has already been noted in other disciplinary areas, a certain concern is instead fed by that part of the doctrine that in the mechanisms of profiling the web and in the use of algorithms predictive has glimpsed the risk of "new discriminatory practices and the attack on fundamental freedoms and informational self-determination of the person through the Big Data and the technical specifications of analysis (HR Analytics)"[9].

The use of more advanced software than the "computerised archives", which at the end of the 1980s allowed "the holding and processing of information on each worker"[10], gives the employer access to an information campaign, useful for taking decisions on the establishment, execution and termination of the contract. This raises fears that some decades ago were already expressed about the computerization of workplaces, enriching the dialectic between the potentialities provided to the production process from advanced analysis techniques and the demands for the protection of workers.

*Autonomous and Robotics systems and* their use on the production chain have been considered by many as a profitable and essential investment, especially in those specific areas in which operational speed and prediction of implementation are essential. Autonomous technology allows machinery and robots to act and behave automatically and autonomously after being programmed to do so. For this reason, in recent years, there has been a profound innovation in the robotic field, with an improvement in various aspects, such as autonomy,

[7] J. Bughin, J. Livingston, and S. Marwaha, *Seizing the Potential of Big Data,* Article McKinsey Quarterly Business Technology Office, October 2011.
[8] M. Weiss, *Digitalizzazione: sfide e prospettive per il diritto del lavoro*, Giuffrè, Milan, 2016.
[9] P. Tullini, *Economia digitale e lavoro non-standard*, Labour & Law Issues, 2016, 2(2), 1–15, in https://doi.org/10.6092/issn.2421-2695/6489.
[10] M.T. Salimbeni, *Nuove Tecnologie e rapporto di lavoro: quadro generale*, in R. De Luca Tamajo- R. Imperiali D'Afflitto, R. Romei, *Nuove tecnologie e riservatezza del lavoratore*, Franco Angeli, Milan, 1988.

flexibility and cooperativity. This mechanism led to a great collaboration between humans and robots, which integration brought a reduction in costs of accessing the availability of this new generation of robots, and at the same time to an increase in their capabilities.

Automation can change the way people work. All occupations have a certain potential for automation: for some activities, they are fully automated and for others only partially. As it is estimated on the analysis developed by McKinsey Global Institute[11], in about 60% of professions the share that can be entrusted to machines is no less than 30% (figure 1.3 describes this trend). And the analysis does not only consider the jobs that consist of the simple execution of routine operations: we live in a new technological era in which robots and computers are increasingly able to perform tasks that require cognitive skills.

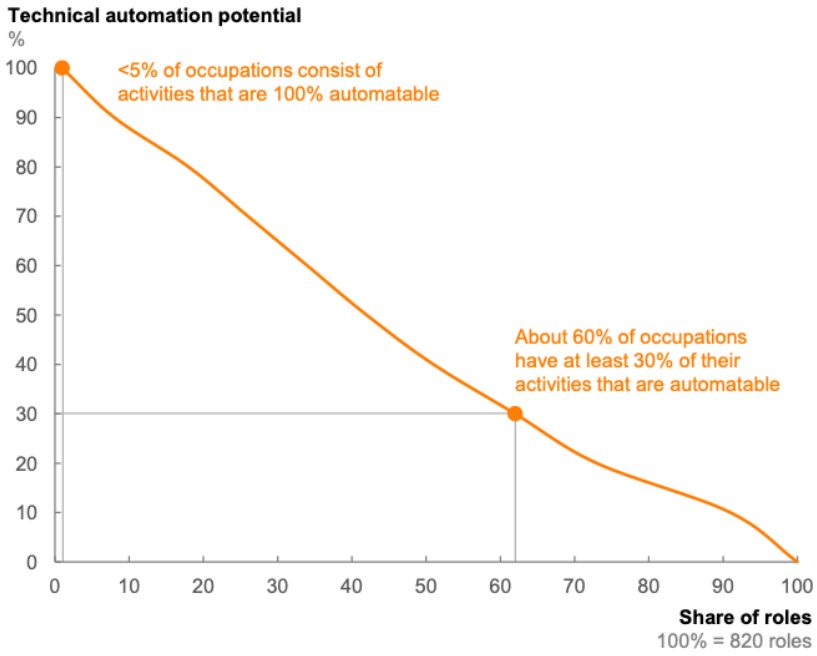


Figure 1.3: Report McKinsey Global Institute

The pace and scope of automation, and therefore the impact on workers, may vary between different activities, professions, wage levels and skills. The jobs which can be automated first are those involving physical activity (particularly in manufacturing and retail) and those involving data processing (collection and processing). Some forms of automation can also affect skills, increasing the productivity of highly skilled workers. The study estimates

[11] Report McKinsey Global Institute, *op. cit.*

the percentage of time savings made possible by automation for the main professional categories (shown in percentage in Figure 1.4).


Figure 1.4: Report McKinsey Global Institute

The potential for automation is not necessarily linked to the low-paid professions: there are workers with low wages who cannot be replaced by machines, just as high-paid roles are susceptible to some degree of automation.

Much of the current debate tends to highlight the risk of widespread unemployment that could result from automation: instead, McKinsey analysis[12] shows that, due to the ageing of the population, a deficit is much more likely in the coming years than a surplus of human labour. The changes in the workforce generated by automation technologies are comparable in size to those experienced by developed countries in the 20th century in the transition from agricultural to industrial economies. Those changes did not result in mass long-term unemployment because they were accompanied by the creation of new types of work not foreseen at the time. The analysis shows that humans will still be needed in the world of work: total productivity gains are estimated to only come if people work alongside machines. The study emphasises rather the positive role of automation in helping to bridge the gap that the deficit of working units contributes to creating compared to the expected growth.

*The industrial Internet of Things* also denoted as “IoT”, can be considered as one of the main drivers of Industry 4.0. It represents the use of the internet to connect different devices, users, and machines to guarantee accurate observation and control over the right functioning of machines and the transport of products. The Internet of Things has a central role in today's reality since the level of complexity reached today could not be managed by the previous industrial systems. The new systems which include new digital devices allow instead the

[12] P. Tullini, *op. cit.*

correlation between a traditional physical system, which must not succumb, and a new virtual world to ensure coordination between different devices.

The Internet of Things enhances numerous economic advantages since it improves operational efficiency and therefore production, allowing to reduce in costs and time consumed, since coordination is more efficient and faster where the analysis of activities and processes of decision-making is decentralised. The interconnection guaranteed by the Internet of Things, which connects all technologies and devices, allows for obtaining faster solutions whenever a problem arises inside a production process. Moreover, “IoT " not only reduces the time and costs of production but also permits new advantages in terms of production and its quality, since there is greater availability of these technological tools due to the reduction of their cost and the ease with which experienced engineers can implement them.

In the industry field, the Internet of Things had a significant impact on the value creation of enterprises, which also allows influencing the creation or modification of entire business models improving the basic functions of a product also through the addition of digital IT services such as to upset the product and the whole way of doing business.

Digital technology has not only transformed factories, the skills needed for workers and some of the oldest professions in the world but also changed the way they do their jobs. Thanks to the development of the Internet of Things and the progress of digital, a new way of working, that is, smart working (agile work), has begun to be increasingly widespread in companies around the world. Before talking about smart working specifically, it is appropriate to define what is meant by telework, which is the starting point for the birth of agile work. The term telework refers to work that takes place at a distance from the headquarters, a practice that began to spread in the United States around the seventies thanks to the development of information technology and telecommunications[13].

As already mentioned above, smart working arises from telework but differs from the latter; in fact, "smart working represents the evolution of telework, made possible by the innovation of digital tools and the spread of connectivity"[14].

Smart working and telework represent two working modes that are conceptually different but nowadays, they are in a continuous phase of evolution and are being adopted by an increasing number of companies since they offer advantages in terms of savings on fixed costs and increased productivity. Smart working allows the worker to carry out their activities

[13] Definition from the Cambridge Dictionary in https://dictionary.cambridge.org/dictionary/english/teleworking
[14] S. Chieti, *Che differenza c’è tra smart-working e telelavoro*?, in: https://www.quindo.it/telelavoro-e-smart-working/, 2021.

outside the company and to decide independently the time and place of work, so they can work from home, in a bar, in a hotel room or even in the same company, in spaces specially dedicated to the so-called "co-working". It is important to stress that agile work does not represent a new form of work contract but rather a new flexible way through which the employment relationship is performed in which relations between employer and employees are regulated by normal employment contracts that align them both in regulatory and wage terms with insiders, or those workers who perform their duties within the company[15].

*Cloud Computing* is a centralization of the storage of fundamental data and information at companies. It indicates the set of services offered on demand from a supplier to a consumer using the Internet. Cloud computing appears to be a service provided by third parties for important parts of computer operations according to methods, time and costs established by the users themselves who give up the possession of their own hardware and software resources by acquiring them through a simple internet connection according to their needs. The adaptation of a “cloud” infrastructure for archiving data collected can have positive consequences in the overall history of a business.

Besides the good side of having a cloud, it also has a big critical issue which regards the security of data. This does not only imply the risk of a loss of full control of their data and resources, but also the risk of oligopoly with the centralization in the hands of a certain number of companies where data no longer resides in a single hard disk, but they are increasingly remote elsewhere.

Moreover, this enabling technology brings great help to manage the new working trend just mentioned, smart working, since it gives the possibility to manage workers and work itself through the network. The cloud, like smart working, allows people to manage their activities and their relationship with customers and consumers remotely.

[15] M.T. Salimbeni*, op. cit.*

### 1.2.2. Control on Work Activities

As we have just analysed, many new technological tools have started to be used in the context of employment, leading to a drastic shift from a traditional world, to a more technological and digitised one.

Alongside the evolution of these innovations, new instruments related to the control of work have also been developed, as we have previously anticipated, principally based on the analysis of the huge amount of data generated as a succession from the last industrial revolution. These new control tools can be of different types, sharing the general function which is the possibility for employers to constantly monitor their employees.

"Employers have always collected information on their employees, both at the pre-contractual stage, to select the partners and contractors, and at the enforcement stage of the obligation, to protect its interest in the proper performance and for other purposes that could not be considered as the legal effects of the employment contract, but had relation to the enterprise organisation as a power structure"[16], only that, compared to the past, the increase in levels of automation in the organisation of work has made it possible to refine the techniques through which employees can be controlled, and consequently the space between a control has been reduced the protection of the entrepreneur's interest in the proper performance of the service and protection of other purposes.

It is easier to fall into this risk if one observes that it is now all too easy for the employer to control his employee through the use of new technologies. Precisely, because the relationship between man and machine becomes ever closer, between the performance of work and technologies applied to production processes, with the consequence that it is necessary to assess whether the legislator, who can only follow such social phenomena, has put in place effective rules and limits to a control on the potentially unrestrained work performance.

The relationship between man and machine can determine the dual effect of replacing the former with the latter or complementarity between the two: in the first hypothesis the advantage is to relieve the physical fatigue of human activity, which is replaced by the work of

[16] M. Barbieri, *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse*), Volume Controlli a distanza e tutela dei dati personali del lavoratore, edited by P. Tullini, *Turin, 2017, pp. 183-208.*

the machine, but on the other hand, the trend towards fungibility between human intelligence and the artificial door represents an undeniable threat to existing employment levels (already bleak); in the second hypothesis, that of complementarity, "the most immediate fallout concerns the realisation of the object of the employment relationship: the fulfilment of the service"[17], that is, in practice the boundary between the obligations of the provider of the work and the rights of the same runs the risk of becoming blurred.

If the worker uses technological tools to render the performance, on the one hand, this allows him to execute his obligations more quickly and efficiently, for the benefit of the entrepreneur, on the other hand, the machinery to which you are referring is often suitable for gathering information which is useful for the employer to measure performance, as seems to suggest the story of the electronic bracelet made in Amazon, which will be analysed on the following paragraph.

The pervasiveness of new technologies allows you to monitor all the behaviours of workers while they work and not only those related to the performance of the service. Thus extending on facts also substantially unrelated to this, in the opinion of those who write in Art. 4 of the Workers' Statute[18] contains rules that allow us to frame the legitimate expectation of the employer to adapt the production environment to the introduction of new technologies, on the one hand, and at the same time, to guarantee working people that the control legitimately exercisable by the employer is kept below the threshold of "legally permissible", a threshold that can now be determined also by reference to the c.d. Privacy Code and, in general, to the European standards. In this perspective arises the story of the electronic bracelet patented by Amazon, for the understanding of which it is necessary to retrace the stages that have marked the progressive evolution of the statutory norm in a matter of remote controls of the activity of the workers.

In Italy, there is not much documentation about the issue of new technologies of control in the workplace by either scholars or by unions[19]. On the other hand, studies, analyses and documents on the quantitative dimensions of the phenomenon have been produced in the international context for some time. For example, in the United States, the American

[17] P. Tullini, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa, in Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, Turin, 2017, p. 6 ss.
[18] Article 4 of Workers' Statue, *Impianti Audiovisivi e altri strumenti di controllo.*
[19] For a general reflection on these issues see also M. Paissan, *La privacy è morta, viva la privacy*, Ponte alle Grazie, Florence, 2009.

Management Association produces and distributes annual reports on electronic surveillance in the workplace[20]. The results of the survey for 2007 show that 70 per cent of employers monitoring employees' Internet browsing by recording and storing content; about 30 per cent of workers were reprimanded and suffered some consequences for illegitimate use of email and the Internet; 10 per cent monitored blogosphere and social networking looking for comments about the company; almost 50 per cent monitor phone usage and in 20 per cent of cases record phone calls or messages left in answering machines. In Italy, there are no similar surveys, but it is reasonable to assume that here too the increasing availability of increasingly affordable technologies has led to the spread of this type of control.

In our country, we have a regulatory framework which, in terms of principles, establishes high guarantees, much more than elsewhere, thanks to the Workers' Statute[21]. On the other hand, for some, the overall picture, as we shall see, presents some uncertainties.

Let's consider the new control tools, widespread in Italy. This is the case with GPS, which allows the geographical position of the worker at all times (think in particular of people driving vehicles)[22]. But also, RFID[23] (Radio Frequency Identification, able to track people and things) or microchips to be inserted under the skin of employees (it happened in the United States). Or systems capable of recording the sequence of keys typed at each workstation (such as and how many per minute), or of reproducing and recording what is displayed on the worker's screen, or of following and recording the Internet browsing performed (com-taken therefore the visited sites), or to record both the external data and the content of the e-mail sent and received by the terminal supplied (both on the institutional account and on that, if any, private).

New control technologies are now readily available and affordable, if not derisory. Their characteristics are invisibility, systematisation, and the possibility of acquiring information not only about working time but also about the lifetime of the employee.

In the face of such pervasive perspectives of technological control, over and above the inevitable considerations of the dubious legitimacy of these systems, account must also be

[20] The 2007 Electronic Monitoring & Surveillance Survey is co-sponsored by American Management Association (http://www.amanet.org) and the ePolicy Institute (www.epolicyinstitute.com). A total of 304 companies participated: 27% represent companies employing 100 or fewer workers, 101-500 employees (27%), 501-1,000 (12%), 1,001-2,500 (12%), 2,501-5,000 (10%) and 5,001 or more (12%).
[21] The Workers' Statute (Law 300/1970) sets out rules to protect the freedom and dignity of employees, trade union activity in the workplace and rules on employment.
[22] Garante Privacy, n. 1531604, *Trasporto pubblico: geolocalizzaione e sicurezza dei passeggeri*.
[23] Garante Privacy, n. 1109493, *Etichette intelligenti (Rfid): il garante individua le garanzie per il loro uso*.

taken of the consequences on the working environment itself. Numerous studies[24] (in the USA, Great Britain, and Australia) invariably attest to the increase in stress, and anxiety but also the overall worsening of the quality of relations, and attrition of mutual trust between employees and managers. In short, negative results on all fronts. The "ease" of some technological controls, perhaps accompanied by more traditional systems, has also led to resounding events[25].

For this reason, the following analysis will mainly focus on the protections that relate to the processing of personal data in the employment context and how these protections have been adjusted to the drastic technological changes enhanced by the advent of the fourth industrial revolution.

#### 1.2.2.1. The Amazon Case

The event of the electronic bracelet patented in January 2018 by Amazon has taken on importance in Europe[26], to impose on the interpreter delicate problems regarding the legal effects of the decision of the American company. In practice, this instrument emits ultrasonic sound pulses and radio transmissions that allow the company to understand where the hands of the employee are. Compared to the past, when employees were using a small scanner to control company inventory, Amazon decided to move such equipment on the wrists of employees, to leave their hands free and can therefore take the product from the warehouse and box it in less time[27]. The bracelet, moreover, geolocates[28] the employee and through a countdown that appears on the device provides him with the maximum time to reach the location of the next product to be taken from the shelves.

[24] G. Harrison, M. Lucassen, *Stress and anxiety in the digital age: the dark side of technology*, the open Learn University, UK, 2019.
[25] P. Tullini, *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro: uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali,* Volume 58 of Treaty on commercial law and public economic law, Cedam, Padua, 2010.
[26] See, for example, articles published in well-known European newspapers, such as: https://www.theguardian.com/technology/2018/jan/31/amazon-warehouse-wristband-tracking.
[27] M. Fcault, *Sorvegliare e Punire, nascita della* prigione, Einaudi, Turin, 1975, p. 164.
[28] A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori,* in Rivista Italiana di Diritto del Lavoro, 2016, pp. 513-546.

If the employee is "slower" than the time that the Company considers useful to move from one location to another, these could potentially be subject to a disciplinary sanction caused by poor performance. The worker can also insert breaks from work in the wristband, but here too the company allocates the maximum time of the break, depending on the reason why the employee registering it requests it.

In short, the Amazon bracelet seems to be just one of those tools "in which the technology directs, scans and records individual operations, prevents errors and defects, corrects in real time the mode of performance: employees can be completely heterogeneous directed by the intelligent system that automatically knows the next step, and sets the next task with extensive predictive capabilities, calculating the operation to ensure quality and control and eliminate manual logging"[29];

It has been stated that the information collected by the bracelet "can be used for all purposes related to the employment relationship" provided that the employee is given adequate information about how to use it and "in compliance with the provisions of Legislative Decree No. 196 of 30 June 2003"[30].

This topic has generated many discussions among politicians[31], but The Italian Ministry of Labour replied with an interesting quote in a press release[32]: "The Jobs Act has adjusted the regulations contained in the Workers' Statute, which date back to 1970, to the technological innovations that have occurred in the meantime. And so, the regulation has not 'liberalised' monitoring, but has clarified the concept of 'remote monitoring tools and the limits on the use of data collected through these devices, in line with the indications that the Data Protection Authority has provided in recent years".

This paragraph just wanted to highlight an example of how a control tool, released after Industry 4.0, might generate debates in the privacy context because it is too pervasive in each worker's private sphere. Then the concept of "control at work", and how far it can go to be lawful, will be discussed in the last chapter.

The future will see more and more, even in the field of work, complex interactions in the human-machine relationship. If this is unavoidable, what problems will it entail in the representation of the individual and his experience? It is not so much a problem of

[29] P. Tullini, *op. cit.*
[30] M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, CSDLE It., n. 300/2016, p. 7.
[31] Article from The Medi Telegraph: *Never in Italy, to amazon and its bracialet*, 2018, in: https://www.themeditelegraph.com/en/transport/intermodal-and-logistics/2018/02/03/news/never-in-italy-to-amazon-and-its-bracelet-1.38085393
[32] M. Marazza, *op.cit.*

unemployment as of possible "dehumanisation" of work and its meaning. This is also about the time and quality of work. The challenge of combining efficiency and reduction of fatigue with human times and modes of life will be the cornerstone for an evolution towards a better and differently anthropogenic world or, on the contrary, for apocalyptic scenarios.

### 1.2.3. Benefits and Challenges

Industry 4.0 has brought many benefits such as increased exponentially productivity, efficiency and quality in the production process, satisfaction of consumers by focusing more on data and so more on people's needs, easier decision-making with data-based tools and increased competitiveness in the market. We could split into four categories the most relevant benefits that this last revolution brought.

The first category will be the manufacturing one since it has been the sector most affected by technological changes. Increasing productivity, less machine downtime, deeper levels of integration, automatic track and trace processes, optimization of the supply chain since it is all connected and this enables real-time monitoring, and higher flexibility to respond to changing markets. Thanks to the big amount of data and the automated technologies available, employees have been empowered. They can focus more on adding value to activities instead of focusing on repetitive tasks that now machines will oversee. With the development of production lines and business processes the collaborative and sharing work has drastically increased, since everything is connected regardless of location or time zone.

The second category to consider will be the one related to quality and compliance. With the new technological tools, it is possible to automate compliance, including quality inspections, track, and trace and more. Moreover, the same concept applies to improving the quality of a product, since it is now possible to move the quality step in the production line. Besides reducing time-consuming during the process that before was taking place in the "inspections room", it allows us to check the quality before reaching the failure stage so this will reduce waste and save time and costs that for huge amounts of items make much difference. Moreover, this automated process will reduce human errors during the quality step and automate the collection and storage of data.

As the third category, we consider all benefits for customers and patients. Thanks to the collection and storage of data, personalised products can be created and therefore the customer experience will increase. Nowadays products are also becoming more intelligent since with sensors, 5G and the industrial internet of things it is possible to connect multiple products that can share multiple information for instance: patient health data to enhance diagnosis and treatment, product data to help Research and Development to develop improvements and usage of data to monitor the performance of the device.

As the last category of benefits related to Industry 4.0, we consider all the operations benefits. With the introduction of the smart factory, costs and time spent on products drastically decrease for the following main reasons: less resources, material and product waste, faster manufacturing, lower maintenance costs, lower operating costs, better use of resources and innovation opportunities. The data collection improved the decision-making process since by operating with smart manufacturing processes machines and systems are more integrated and therefore data can be captured and used by the way, enhancing automation even further. So basically, the reduction of costs and time consumed has increased revenues, profitability, and quality. To exploit all these benefits, it is essential to stay competitive in the market and be always ready to adapt to new changes and new regulations because the world will always be in continuous improvement and staying competitive is an essential requirement.

Besides the numerous advantages that have been listed above, as with any industrial revolution, it has also enhanced many challenges and drawbacks which are principally related to inequality, cybersecurity risk, data protection breaches, high competition on the market and ethical issues.

To adapt to all the technological changes implemented by Industry 4.0, people need to deal with specific technological infrastructures and need to learn various technological skills, and already by now this mechanism might generate inequality since not all people in the world can have such infrastructures or skills available to learn. This inequality leads to discrepancies in terms of income since people with no education or no confidence in technology for instance are directly excluded from most job opportunities.

Another aspect to consider as a drawback is the concept that everything is nowadays connected, so the risk of hacking the data has become very dangerous. Hackers started to steal data and personal data from people to use them for malicious intent or to sell them to other parties for marketing purposes for instance, and this leads to a lack of privacy on personal data that will be analysed in more detail in the second chapter.

Carissa Veliz[33] states: "The most troubling victim of Google's advertising success, as you can imagine, was our privacy […]. Google successfully turned data exhausted into gold dust and inaugurated the surveillance economy as one of the most lucrative business models of all time". These quotes make us think about the level of importance that data has, how expensive they should be since they provide important information for many companies' scopes, and how they are instead just stolen from us in a way that we do not even realise.

Related to the latter challenge, we can mention the same issue just examined in the above paragraph, which is the one related to the pervasive control tools nowadays available to control workers. There is a risk of misuse or abuse of digital technologies that could affect workers' rights to privacy and data protection, especially in remote work situations; a risk that your employer will use surveillance and surveillance technology for unintended or unauthorised purposes; digital technology will make surveillance and surveillance processes less visible, pushing the boundaries of acceptable and legitimate surveillance; may increase power asymmetries within the organisation surveillance practices reduce job autonomy and trust in management, affecting employee motivation and employment relationships; excessive or continuous monitoring can be counterproductive, causing employee resistance and non-compliance, ultimately reducing productivity and damaging a company's reputation[34].

Other challenges arise from the level of competition reached after the fourth industrial revolution, such as Netflix competing with movie theatres, Uber competing with Taxis and Airbnb competing with the hotel industry. Innovations and technological changes have increased the possibility to do everything online, without the need of contacting anybody directly. And this process, besides being much faster and being done from anywhere, is also cheaper than traditional industries, so this mechanism is disrupting some of the core industries. This mechanism leads to a drastic shift in the employment context if in the past the only way to plan a holiday was to consult a travel agent, nowadays thanks to easy access to the internet, people started to plan by themself since the web offers thousands of options. So, physical travel agents will probably be completely substituted by online travel agents, which are available even directly on mobile phones.

[33] C. Veliz, *Privacy is Power*, Penguin Random House, London, 2021.
[34] S. Riso, *Monitoring and surveillance of workers in the digital age*, European Foundation for the Improvement of Living and Working Conditions, in: https://www.eurofound.europa.eu/data/digitalisation/research-digests/monitoring-and-surveillance-of-workers-in-the-digital-age, 2021.

The last drawback to mention is inherent to ethical issues, which differ from individual to individual. The most common concern is related to the amount of data that a company has and could steal from people and manipulate them on purpose. For sure the scandal of Cambridge Analytica in 2018[35], when they collected personal data of users from Facebook without asking for their consent and used it for political advertising scope, it has increased exponentially the level of concern of the entire population.

"Personal data is dangerous because it is sensitive, highly susceptible to misuse, hard to keep safe, and desired by many - from criminals to insurance companies and intelligence agencies. [...] Data is vulnerable, which in turn makes data subjects and anyone who stores it vulnerable too"[36]. The author wants to underline how vulnerable people are when they share private information, how hard it is to keep them safe and to remember that the world is full of people/institutions that want your data.

## 1.3. Work 4.0

The fourth industrial revolution determines, therefore, the fusion between the real world constituted by machines, products, places and people, and the virtual world created by the Internet of Things. As has been already mentioned above, this transformation has drastic repercussions also on the employment context.

It was reported how, the term industry 4.0, is intended to refer both to a set of new technologies and new inputs, but also to new work organisations which are intended to bring decisive changes in the way of production and relations between economic actors, including consumers, with significant effects on the labour market and on the organisation itself[37].

This fusion between reality and digital creates in the production field the so-called "smart factory", which is a factory where the way of conceiving production changes, less standardised and increasingly faster and more personalised, able to meet the needs of each customer,

[35] More information on the CNBC website: https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html.
[36] C. Veliz, *op.cit.*
[37] A. Magone, T. Mazali, *Industria 4.0. Uomini e Macchine nella fabbrica digitale*, Guerini, Milan, 2016.

considered no longer as a group of people (mass production), but rather as an individual with specific needs; all this in a place called Cyber-Physical System, in which the entire production process assumes the self-diagnostic ability to detect errors and possibly correct them. This industrial process is based on robots which replace workers ("blue collar"[38]) on the assembly line, to perform manual work more efficiently, and skilled workers ("white collar"[39]) saw a reduction in their duties as a result of the introduction of new technologies.

The consequences of Industry 4.0 on the world of work are not only limited to changing the job, skills and roles of professionals but also working hours and workplaces. The new organisation of work does not always require the physical presence of the worker because, thanks to the new technologies and increasingly faster internet connections, it is possible to perform some tasks in places far from the physical headquarters of the company, using a PC or even a Smartphone, as defined above under the definition of "smart working".

The new organisational trends, the evolution and diffusion of technological and information tools, change, day after day, the working processes and highlight, more and more, how the nature of work is changing and how companies are looking for an increasingly flexible solution. The answer to all these needs can lie behind the introduction of innovative approaches to work organisation, which are characterised by flexibility and autonomy in the choice of spaces, working hours and utility tools in the face of greater responsibility for results, based on a strong cultural change.

A clear example arises from the new economy called the "Gig Economy", in which workers started to deal with business contracts completely established on the Internet and started to focus more on short-term contracts compared to the long-term traditional ones.

The concept of the "Gig Economy" started to develop back at the time of the first industrial revolution, and since then it has been continuously changing and adapting alongside industrial revolutions. During Industry 1.0 labour patterns changed due to the discovery of steam engine technologies, and so they were able to accelerate processes and therefore generate massive productivity gains. Then during the ages of Industry 4.0, with the development of artificial intelligence and automation skills, the concept of the "Gig Economy" started to adapt and therefore to be digitalized and automated as well. Today under this concept we include all

[38] Definition of Blue-Collar from Investopedia: *the term blue-collar worker refers to individuals who engage in hard manual labour, typically in the agriculture, manufacturing, construction, mining, or maintenance sectors*.
[39] Definition of White-Collar from Investopedia: *White-collar workers are often found in office settings. As the name implies, they are generally suit-and-tie workers who wear white-collared shirts. Their jobs may involve working at a desk in clerical, administrative, or management settings. Unlike blue-collar workers, white-collar workers don't have physically taxing jobs*.

those short-term contracts that can be established exclusively on the Internet, and some of them are even fully completed through the Net.

The factors of growth are related to flexibility, comfort, and price, since by connecting consumers and suppliers directly, many services in between which are known as secondary costs, can be cut out. As also the workforce in the company is feeling the digital transformation, it needs every day to implement an innovative business model of human management, and many freelancer employees started to prefer temporary jobs to long-term ones. Following this behaviour, companies must adapt to workers' needs and therefore offer remote-work platforms to allow workers to work from any part of the world.

## 1.4. The New Employment Relationship

As previously anticipated, digitalization and technological developments have direct implications for labour markets, together with many other aspects such as demographic development, globalisation, competition but also climate change. Some of them might guarantee a positive impact on the labour market, on the contrary, some others can be more disadvantageous.

It should be noted that the innovation of Industry 4.0 involves a substantial change in the skills and abilities that every worker, present and future, must possess to face this revolution without serious consequences. Technical skills will no longer be enough, the workers of the future must also have skills defined as "transversal" (soft skills). These relate to the ability to solve a problem, creativity and the development of critical thinking. All these capabilities will allow us to better adapt to a rapidly changing scenario, so it is crucial to be ready to catch the benefits of Smart Manufacturing, and digital innovation in industrial processes.

The employment relationship is constantly changing due to technological innovations that our world has been through and will go through in the future. The Gig Economy, as previously mentioned, is the new term assigned to a new way of dealing with employment. This latter is an economic model based on work on call, occasional and temporary. From there, companies

can hire independent and freelance contractors to support full-time and permanent employees. The Gig Economy can bring great advantages to companies because it is a model that responds to today's work market, increasingly flexible and digitalized. It refers to the concept of using online platforms (apps) to perform job activities, which are usually "short-term contracts" and can be done locally or remotely.

Expanding the definition in a modern way, it can be said that the gig economy is formed by the set of platforms that connect demand and supply of gig and work on demand using technology and in particular the internet. It is essential to underline the crucial importance that the development of the internet has had in the formation of this new type of market: without online platforms, the gig economy could never have developed quickly and consistently since the encounter between workers and companies would be much longer and complex.

In particular, the first modern mover in this field was Amazon which created the first platform for the encounter between demand and supply of gigs in 2006 which is called Amazon Mechanical Turk. Through this platform, the American multinational had the goal of solving problems related to some algorithms that could not operate efficiently making slow and cumbersome even some elementary processes. The idea at the base was to implement a new type of outsourcing at a very low cost letting a large mass of people solve mini tasks characterised by a low level of difficulty and a high degree of volatility. The ultimate goal was undoubtedly not to hire new employees who would increase operating costs. It didn't take long to see the potential of such a platform. Soon, the range of tasks that could be performed through Mturk was extended, ensuring a high level of efficiency.

Later also moved the first competitors including Deliveroo in the field of catering and Uber in the transport of people thus giving way to the real gig economy. However, it is not correct to assume that the only need for efficiency is behind this change. While it is true that this need has become dominant in the modern world thanks to the continuous technological evolution of recent years, we must not forget that a phenomenon of this kind has even deeper social and cultural roots.

This phenomenon started to develop thanks to the combination of already established self-employment or on-call work, with the new digital developments coming from the fourth industrial revolution. Three parties are involved when dealing with this contract: the platform, the worker and the client who is the one requesting a specific task, and it can be either

"crowdwork" or "work on-demand via apps" which differs in the way the job is provided, physical or virtual, and for the working location, local or at the global level.

### 1.4.1. Gig Economy Preconditions

The main effects of the digitalization of work were the birth of new organisational paradigms, heterogeneous and subsumed in the macro-categories, variously called, sharing economy, gig economy, platform economy, and economy on demand, whose most relevant and known phenomena are those of crowd-employment (c.d. also crowd working) and call-work through digital platforms (c.d. work on demand). An archipelago of new forms of the economy has emerged, with new subjects and as many unusual contractual relationships between the social and legal actors involved.

Fundamental features of these new organisational models are the use of computer tools for the meeting of supply and demand and the performance of work, the constant and physiological use of electronic tools of work, particular and incisive forms of remote control through mobile devices and the exploitation of ubiquitous technologies, as well as transaction costs reduced to a minimum with a view to maximum efficiency.

To completely understand the concept of the gig economy, it is worth explaining which preconditions are related to it, otherwise, people might just see the gig economy as a particular market shaped by technological factors. Woodcock and Graham[40] identified nine important preconditions that are connected to factors of society, technology, and political economy.

The *first* precondition relates to "platform infrastructure" which presents rapid growth due to the availability of technology such as the one developed by the fourth industrial revolution. One of the most well-known gig economies has been Uber's platform, which works as an intermediate platform able to connect people looking for rides (buyers) and riders (sellers). Gig economy companies are not employers but a bridge between supply and demand, so they are

[40] J. Woodcock, M. Graham, *The gig economy: A critical introduction*, Polity, Cambridge, 2019.

classified as technology companies, and not as taxi or delivery companies. Platforms connect the two parties, which might lack proximity or synchronicity, through negotiation-based matching: in which parties post information about their skills; and static-price matching, in which prices are fixed and thus there is no negotiation.

The *second* precondition relates to the "digital legibility of work", so the concept of measuring work on digital platforms. In many cases workers are monitored, screens are recorded, and real-time location tracking is used, so that it is possible to have many details about a worker's performance and therefore evaluate them better. For sure actions that might be very useful for employers, but maybe less fair if we consider the employee's point of view. We will analyse more in detail this "privacy" concept in the next chapters of the thesis.

The *third* condition relates to "mass connectivity and cheap technology", which refers to both the social and technological aspects. The Internet connection is a fundamental pillar of modern society since without active connection digital platforms are not available and therefore, any process related to the gig economy will not work. Nowadays, over half of the world's population is connected to the Internet, and 5.16 billion people are Internet active users worldwide, which is around 64.4% of the entire population[41]. However, digital asymmetries remain real since the percentage of the population which has access to the internet in advanced countries is much higher compared to the population in developing ones. The element in common between either low-, middle- or high-income countries is the use of mobile phones to connect and no longer dial-up models. Gig economy firms are much more facilitated by innovations in the technological field that are cheap enough to mass uptake so that it is possible to include a wide number of clients and workers. In some cases, firms focused on "global services ", which are platforms that enable mass migration of labour. Workers are placed in competition with each other on those platforms, and by doing so, clients will have a wide variety of workers to choose from.

The *fourth* precondition focused on social aspects "consumer attitudes and preferences". To attract consumers and engage them in these online platforms, a degree of digital literacy and practical skills in using technology for many daily activities is needed. Some platforms are built on existing markets, so in this case, it will not need a significant change in consumer

[41] Report Digital 2023, *I Dati Globali, We Are Social*, https://wearesocial.com/it/blog/2023/01/digital-2023-i-dati-globali/.

behaviours. But in the case of industries dealing with new demands, activities offered must be attractive, and meaningful and must make sense to consumers.

The *fifth* precondition is "gendered and racialized relationships of work". When considering this social precondition, we principally refer to the inclusion and exclusion of women in different jobs, even when considering the gig economy. This issue is generally followed by a gender gap and fewer social protections towards those individuals. Besides the gender gap, racialization is another issue that involves migrant workers and minorities. The combination of these two issues might generate an exploitative workplace not protected by any regulations and thus, impacting weak workers negatively.

The *sixth* precondition is the "desire for flexibility for/from workers", based on the concept that both workers and employers do have the desire for flexibility. Gig workers prefer to be engaged in short and repetitive tasks rather than long and complicated projects, to reduce the boundaries of the local market for instance and exploit the flexibility that the gig platform guarantees. We will see more in detail, in the following analysis, that flexibility is not always a positive aspect, because in many situations could be a drawback. Gig economy platforms are not considering workers as their employees, but they consider them as independent workers, and by doing so, they remove all the responsibilities over them. This has many disadvantages that make people evaluate whether "flexibility" has a positive or a negative impact on gig economy workers.

The *seventh* precondition relates to "state regulation", and so it refers to the concept of political economy. There is a long history behind this precondition since it relates to all the political situations until our days. We can start from the financial crisis of the 1970s, and the structural crisis that followed up. In this contest, even the "standard employment relationship" was under threat since inflation and unemployment were growing. Yet, the crisis allowed coming up with a new market-oriented reform called "neoliberalism": the ideology behind this concept is the one-off reducing the state interventions for economic and social activities, and deregulation labour, financial markets, commerce, and investments. Investopedia gave the following definition "A policy model that encompasses both politics and economics and seeks to transfer the control of economic factors from the public sector to the private sector"[42]. So basically, the main idea was to reduce government intervention and regulation, and some of

[42] L. Manning, *Neoliberalism: what it is, with examples and pros and cons*, in: https://www.investopedia.com/terms/n/neoliberalism.asp, 2022.

the famous initiatives have been free trade, globalisation, and reduction in government spending. This period has completely shaped the current state of the employment relationship, and the labour market has been deregulated. However, after the financial crisis of 2008, neoliberalism lost its force. The following years have been subject to insecure and low-paid work, and many changes in terms of the welfare state. Even if neoliberalism ended, many countries are still looking at the gig economy as a potential source of using some of the ideologies used in the past. Thus, for the growth of venture capital, the gig economy became the perfect outlet.

The eighth precondition relates to "worker power", so, still related to political economy. The political trend previously mentioned has weakened employment protections, increasing the instability in terms of contracts of the labour force. In most of the gig economy, workers are missing many protections and regulations that regular workers have. Working power, in this context, refers to the power of existing labour movements and how their power can change and re-design the environment in which platforms operate.

The *ninth* precondition involves "globalisation and outsourcing". Globalisation has led the world to become interconnected and to exchange knowledge around the world, and thus, it allows the spread of technological infrastructures which allow the internationalisation of working practices. Then, outsourcing, allows people to work completely from remote platforms, and the integration of firms in different economies, which is the concept on which the gig economy is principally based.

### 1.4.2. Crowdwork and Work-On-Demand via apps

"Gig economy" has caused many debates about the nature of the job, the relationship between the three parties involved and the working conditions of employees, because, as previously anticipated, the job of on-demand workers is principally based on algorithms and on the data, which is a completely different concept than the one that applies to the traditional employee. Some of the most famous examples relate to all the transportation companies such

as Uber, which connects the driver with the passenger through an online platform, and to all those food delivery companies, which oversee delivering food about what the client selects from its web application. In this subchapter, we will make a distinction between Crowdwork and Work-on-Demand via apps, which are two different categories applying to the area of the gig economy. The common characteristics are that they are both supported by digital technologies to match demand and supply and they are both flexible in the context of working conditions.

The category of crowdwork refers to the activity of outsourcing specific tasks to a geographically dispersed crowd through the Internet. This platform involves three actors: the online platform, the crowd sources which are its clients and the crowd workers which are its registered members.

The first actor has the role of intermediation between the other two parties, the clients overseas outsourcing specific tasks to the members, and the requirement is that they have a computer and access to the internet. Some examples of the most famous crowd sources are Google, Facebook, Intel, and many other companies of different sizes which want to reduce general costs. Besides these examples which are based on simple and repetitive tasks, there are also different approaches, such as the one offered by Freelancer, in which companies or individuals, who need some help from professionals to complete a specific task, post a complex project on the net and after freelancer's offers are published, the company will be in charge of selecting a freelancer that will be in charge of complete the entire project. In this last case, the crowd workers can select whichever project fits better their knowledge and monetary rewards, but at the same time the offer done by the crowd workers must be selected by the crowd sources, and this last figure can be a company can also ask for specific qualifications or reject the final project if not as satisfied.

As we have seen, when considering the figure of crowdwork, we have two different categories: the one in which individuals are asked to perform micro tasks which often require little time, little knowledge, little reward compensation and which are often repetitive tasks; instead on the other category we have the figures of freelancers in charge of complex projects that require higher knowledge, higher duration, and higher compensation. These small tasks or complex projects can either be assigned to selected individuals or also to a crowd of people and

they are all published on a crowdsourcing platform, that according to author Kagenr[43] the platforms divide into four categories:

- Facilitator platform: in which the client and the worker can directly communicate from the beginning of the project until the end, as freelancers do.
- Arbitrator platform: this includes competition between different suppliers to provide the best possible solution. In this category only the best idea, so the winning solution, will get the monetary return.
- Aggregator platform: in this category, we refer to repetitive and small tasks done by many different workers.
- Governor platform: covers the most complex projects, which require highly qualified workers with numerous skills.

The second category of workers is instead called “Work on-demand via apps" in which the work is provided by individuals in a specific area through location-based applications. So, the first part of the work is done online, but then it is performed offline. In this category, workers have opportunities to work within a geographical limit, contrary to crowdwork in which workers were limitless since not related to geolocation. The most relevant example in this category is Uber[44], which is an online platform that connects the user with the driver in relation to their geolocations. The entire relationship between these two parties happens on the “Uber” application: the driver accepts the user that asks for a specific ride, and then the platform provides the user information about the selected driver with also the expected time of arrival. The price will be decided by the software about an algorithm established, and thanks to another algorithm the user pays through the app, a percentage goes to the driver and the rest to the Uber platform.

The use of platforms allows the client or the employer (depending on the hermeneutic approach chosen in terms of qualification of the employment relationship as self-employed or subordinate) to take advantage of particular monitoring tools, such as geolocation systems, the collection of data on online access, customer satisfaction assessments; tools all derived from the very structure of the platform and the characteristics intrinsically linked to it and the performance rendered.

[43] I. Oshri, K. Kotlarsky, L. Willcocks, *The Handbook of Global Outsourcing and Offshoring*, 3rd edition, Palgrave Macmillan, London, 2015.
[44] Uber platform website: https://www.uber.com/it/it/.

To become part of the pool of lenders on call it is enough to equip yourself with a mobile device with a fast Internet connection and register on the site, adhering to the contractual clauses imposed by the platform, configuring workers as self-employed or even as "partners" of the platform, even though subject to qualitative and quantitative standards established unilaterally by the latter. However, the performance is subject to monitoring and direct and indirect evaluation, since the approval systems impose precise rules of conduct, discouraging any kind of non-compliance. In some cases, providers that are persistently below the minimum standards identified by the platform may incur negative reports or even forced disconnection from the platform.

The new work-focused organisational model through the platform, therefore, presents opportunities and risks at the same time. The former relates to the possibility of carrying out small tasks on a freeway, benefiting from additional income quotas. The risks, on the other hand, concern those who identify work with the platform as the main source of income, since the conditions offered can lead to a high rate of precariousness. But in general, the risks are also linked to the uncertain legal qualification attributed to workers and the weak conditions that apply to them since they are not considered real employees.

Moreover, as will be said below, significant effects must also be identified in the exercise of the power of employer control and, consequently, of disciplinary power. The first in fact becomes more widespread, having the employer access to multiple and heterogeneous data on the number of contracts accepted, the rate of availability and customer satisfaction and constituting, above all, the computer device is an essential tool for the performance of work. All this is the most linear consequence of the combination, in such cases, of the human factor with a high rate of technology.

## 1.5. Opportunities and Challenges

The new opportunities, related to the development of new technological innovations, have enlarged workers' opportunities, increasing benefits but also some challenges. Starting from the advantages from the worker's point of view, we must first mention "flexibility", since it is

drastically increased due to the new digital labour platform. Flexibility permits workers to work when, where, and how they want, and this leads to a better balance between work and life. Another big advantage of working through the net is the opportunity to work on a worldwide basis, especially in the case of the first category previously mentioned, crowdwork.

The gig economy has increased the number of possible jobs available to workers and has escaped the boundaries of local workers' perspectives. Workers can select whichever job is more suitable for them, and this is favourable, especially for people with limitations such as health problems, physical disability, or other issues, who might be otherwise isolated in their homes. So, we could state that the gig economy has given a good contribution to selecting and allocating the right task to the right worker.

If we consider instead the benefits for companies or individuals, whoever plays the role of requesters, the first positive impact arises from the unlimited number of opportunities given by the frequent and continuous demand on the online labour market, since they can choose whichever demand opportunity fits them best. They have, moreover, a wide choice of workers to select, and this possibility allows them to choose workers with high knowledge and skills at a more convenient price compared to hiring these workers inside the firm. Another benefit is the role of information technologies, obtaining information in a fast and cheap way has positively impacted organisations. Moreover, using smart algorithms, the match between the job provider and the work happens much faster and with a better connection. Online platforms are available at any time and place, and this allows companies to always be connected to workers whenever they need them, without limits. This last point might be instead considered as a negative impact if we consider the worker's point of view. A question that might naturally arise is to ask whether freelancers have free time or if they are always connected to the internet platform now that requesters might ask for something at any time.

Is this working condition, of always being "online", better, or worse than the traditional working environment? Freelancers do have a lot of flexibility while working, but they are independent contractors which means that they are not supposed to be safeguarded with labour rights and social protection as traditional employees. Protection and rules do not apply to these workers, so they do not have laws or limitations in terms of working time, minimum wages, holiday, or sick leave. In addition, these workers are mainly centred on opinions, feedback, and reviews, since the platform directly assigns to each person its review given by the requesters, so workers do depend on them.

Workers must perform well to get the best review on their profile, so they must establish a positive relationship with the requester, otherwise, nobody will trust their work. The gig economy, from this point of view, might lack sensitive behaviour towards its workers, since it used to consider them as part of the platform instead of real physical workers. And this behaviour could lead to unempowered workers, as they might feel morally down in the long term since gig economy conditions are often so focused on working online at any time, neglecting human necessities that each worker has. Another dangerous situation is related to the lack of social protection in terms of financial dependence, such as when workers do not register in public institutions for tax purposes.

We have said that the Gig Economy has increased exponentially the job opportunities of workers, but it is essential to focus on which working conditions workers are subject to. Unfortunately, competition between requesters, and workers, is drastically increasing and this leads to the following situation: requesters will try to pay as less as possible workers, trying to minimise wages to save labour costs; on the other hand, workers will have always fewer options to set a fairer price, thus they will be obliged to accept jobs not correctly rewarded or even work for free to obtain positive feedbacks. It might take a long time for workers to establish a positive profile with good reviews on the internet platform, in addition, it also takes a lot of time to look for the right and interesting project before accepting it, and all this time spent will not be compensated.

Another aspect to consider is related to the presence of a deadline for each project on the platform, which differ in relation to the time-zone, and can cause workers to work at any time of the day to deliver the project on time and get positive feedback from the requesters. This mechanism is fully based on reviews and feedback, it does not consider the physical and mental health of a worker and his free time.

Some other crucial aspects are related to the payment process, the unilateral changing conditions by the platform and, last but most important, the pervasive technology established. Payment can create issues for workers because many times are postponed, or even absent from the platform; in some cases, the requester could not be satisfied with the final project to reject the final payment, leading to opportunistic behaviour. This behaviour is completely not correct, but since requesters have the possibility of doing it, and since there are not any rules going against it, nothing will change. Problems arising from unilateral changing conditions can

generate disorders when for instance the requesters change fees of payment methods after the acceptance of terms by the workers.

The pervasive technology is instead the issue that will be analysed the most in this analysis. Workers are tracked anywhere in the world, through GPS or other devices since the platform in which they work is monitored by specialists. When workers are paid per hour, specialists tend to make a screenshot of the worker's current screen to check whether the worker is working or not. The gig economy made people start a huge debate about the role of labour regulations for these "online workers". There have been many different discussions on this topic without reaching a unique solution, since the number of platforms, the different rules, and the different national regulations that apply are several, so it is hard to find a common solution.

To conclude, we have observed that the number of challenges and negative aspects has almost overcome the number of benefits that the gig economy has enhanced, meaning that there is a need to pay more attention and find a permanent solution with the objective of protecting these workers from discrimination and opportunistic behaviours. Because the critical issue is strictly related to the development of digital technology, it does not mean that we cannot use technology as a source of solutions. Because this latter can make huge steps towards a more controlled and protected work environment. Using data-driven technology, for instance, it could be possible to set an algorithm that maximises the time spent by workers to look for the right project.

## 1.6. Privacy and Data Protection after Industry 4.0

The huge amount of data generated by IoT (Internet of Things) devices is critical for companies, influencing important business decisions. Thanks to these technologies, you can improve your quality of life, have richer experiences, and new skills and increase value inexpensively. In addition to these great opportunities and expectations, the emergence of Industry 4.0 presents technological, organisational, procedural, regulatory, and cultural changes and challenges. It is important to solve them collectively because the benefits of greater connectivity, from business to society, far outweigh these challenges.

Among the most complex problems presented by Industry 4.0 is the nature of the personal data that will be used in the organisation of the new production model. In particular, about the implications that these technologies will produce in the workplace, machines, by means of sensors and cameras, can record a huge amount of data, which allows employers to closely observe the workplace and therefore, even indirectly, the workers.

It is therefore important to work to protect the privacy and security of individuals and organisations of all types, giving them the power to choose and control how their information is shared. There is a need to redefine education and training to address the changing needs of the world. Change is inevitable and uncertain and requires innovation and courage. The presence of sensors generates huge amounts of data never generated before. However, it is important to note that this sensitive data includes not only those collected by sensors and then processed but also intellectual property and data that fall within the scope of the privacy legislation.

In the face of this scenario, according to a Deloitte survey[45], about 70% of the manufacturers interviewed exchange personal data to and from the products manufactured and only 55% are concerned with encrypting the transmitted information. The network connection of the devices makes them potentially attachable, especially considering the size of the attacking surface, they could therefore be vulnerable both today and shortly. The careful application of additional security features that include harsh vulnerability tests is now an effective deterrent to most attacks, however, we must make clear that although organisations have the power and duty to reduce the risk of suffering a cyber-attack, none can be considered totally immune.

After this general and introductory chapter, the question which arises spontaneously and which will constitute a reason for investigating this research is whether digitization, in one with the changing approach of organisational models resulting from the increasing use of technological innovations and relocation, the reduced relevance of traditional patterns of working time and the emphasis on the results that the worker must produce in a certain period, constitute a welcome landing place for the labour market; because it is able to combine the mutual interests of the parties to the contract or if, on the contrary, it constitutes the ground for a new conflict, because of the inability of the regulatory fabric to provide effectively deterrent

[45] Deloitte, *Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry*, in: https://www2.deloitte.com/content/dam/insights/us/articles/consumer-data-privacy-strategies/DUP_970-Building-consumer-trust_MASTER.pdf, 2014.

protections concerning the intrusion of the employer in the sphere of privacy and confidentiality of the worker.

It remains to be clarified to what extent and in what way a new regulatory framework can protect the private dimension, since a reassessment of the rights of the worker as a person is inevitable, in order to comply with requests for flexibility which may not be adequately counterbalanced by forms of protection and security for workers.

What must be the subject of research by legal practitioners, continuously and in step with the development of technological innovations, is a new balance between the employer's interest to protect its assets in the face of incorrect use of IT equipment assigned to workers and, more generally, the interest of the employer in the exercise of its power of control, on the one hand, and the right to privacy and confidentiality of workers, on the other. This new and dynamic balancing, however, must be pursued having regard not only to the labour law rules contained in the Workers' Statute but also to the legislation crystallised in the Privacy Code[46], which are now explicitly placed in a relationship of continuous interaction and integration.

[46] G. Finocchiaro, *Limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro, Web e lavoro. Profili evolutivi e di tutela*, P. Tullini, (edited by), Giappichelli, Turin, 2017, p. 60.

# CHAPTER 2 – PRIVACY AND DATA PROTECTION IN THE EMPLOYMENT RELATIONSHIP

## 2.1. The Evolution of the concept of Privacy

The concept of "privacy" has been transformed after the drastic technological changes that Industry 4.0 has enhanced. If in the past the word "privacy" was strictly related to the concept of being let alone and the concept of "personal data" was unknown, nowadays the attention to privacy and data protection has been growing with an increased pace and relevance, due to the technological developments that enable data to flow from one part of the world to another in no time.

Around the 1900s, the concept of "privacy" reached European territory. While the concept of "personal data" is still a long way off, the new concept of privacy is already creating a sense of insecurity in society. So much so that the need to introduce security rules to prevent states from invading their privacy has grown so great that the first legal consequences are starting to arise.

In 1948, the Universal Declaration of Human Rights established for the first time the right to the protection of the privacy of individuals against interference by others, especially states (Article 21[47]). This undoubtedly affected the promotion of individual human rights in Europe, as the protection of personal data was initially guaranteed only as a "right to respect for private and family life". (Article 8 ECHR[48]).

It was not until 1981 that Council of Europe member states recognized a "right to privacy about automatic processing of personal data relating to him ("data protection")"[49] as fundamental freedom. Convention 108 for the Protection of Individuals regarding Automatic Processing of Personal Data is the first and only legally binding international instrument in which European states defined the previous core of rules: a universal standard for all data

[47] Article 21, Universal Declaration of Human Rights, *everyone has the right to take part in the government of his country, directly or through freely chosen representatives […].*
[48] Article 8, ECHR (European Court of Human Rights).
[49] Details of Treaty No.108. Full information: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

processing in the digital domain, which would have been the basis for EU law, treaties and regulations (directives and decisions).

Directive 95/46/EC, adopted in 1995, was intended to "concretize and extend the principles of the right to privacy already contained in Convention No. 108 (of the Council of Europe)" as it was based on the protection of individuals about the processing of personal data and on the free movement of such data[50]. It had taken a cultural debate and dogmatic thinking developed in previous decades and outlined a static model for handling personal data that is now outdated. Technology was different then, since it was a world without many technological tools, and therefore the amount of data collected by electronic devices was much more limited compared to our reality, which is a digital pathway always connected. The current reality of social networks and search engines is in fact based on a model of exchange and aggregation of data and information that was designed from the origin for global circulation.

Thus, for at least 20 years, the right to the protection of personal data has been positively distinguished from the right to privacy.

The right to the protection of personal data consists of the right of the data subject to exercise control, including active control, over that data, a right that ranges from access to rectification. The latter is recognized by the Charter of Fundamental Rights of the European Union, which, by confirming this law, reaffirms some of the principles contained in Directive 95/46/EC[51]. Art. 8 of the Charter mentions as one of the freedoms the right to the protection of personal data, i.e., every person has the right to the protection of personal data concerning him or her. It also states that personal data must be processed fairly, for specific purposes and based on the consent of the data subject or other legitimate basis provided by law, and that every person has the right to access and obtain rectification of the data collected by the company. Always in Art. 8, it is stated that compliance with these rules is subject to control by an independent authority.

[50] European Union Agency for Fundamental Rights, Council of Europe, Registry of the European Court of Human Rights, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018.

[51] The Charter of Fundamental Rights of the European Union, proclaimed on December 7, 2000, was published in G. U.C.E. 2000/C-364/01. Cf. Data Protection Authority, Report 2000, Rome, Presidency of the Council of Ministers, 2001, 262. In doctrine, P. Rescigno, *The Charter of Fundamental Rights of the European Union*, Turin, 2003, A. Barbera, *La Carta europea dei diritti e la costituzione italiana*, in Aa.Vv., *Le libertà e i diritti nella prospettiva europea: studi in memoria di Paolo Barile*, Padua, 2002.

This right is different from the right to privacy, which is included in Art. 7 of the Charter, which affirms the right to respect for private and family life: every person who possesses the norm has the right to respect for private and family life, home and communications.

The right to the protection of personal data is extremely broad, which is a consequence of the same definition of personal data. In fact, the scope of application determined by the definition of personal data is very broad: “any information about an identified or identifiable natural person (‘data subject’); the natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity”[52]. Accordingly, personal data is any information that relates to an individual, including sounds or images. However, anonymous data are excluded from the scope of the legislation. Italian law defines anonymous data as “data which initially or after processing cannot be associated with an identified or identifiable data subject”[53].

Thus, based on the broad definition of personal data, the right to the protection of personal data is the right of individuals to review all information concerning them, which is their reflection and shapes their existence in the information society[54]. The right to the protection of personal data is also known as "informational privacy” or "data privacy", all expressions in which the subject of the right is information or data, although strictly speaking given and information are not congruent terms.

In the Italian legal system, the right to personal data protection was introduced with the law n. 675, 31st of December 1996, "protection of persons and other subjects concerning the processing of personal data" and sanctioned by article 1 of the d. lgs 30. June 2003, n. 196, code on the protection of personal data, reads: "Every person has the right to the protection of personal data concerning him".

[52] The Personal Data is defined by art. 4, n. 1, Reg. UE 2016/679.
[53] Art. 4, paragraph 1, lett. n, of the Code for the protection of personal data has been repealed by d.lgs. 101/2018. On anonymity, please refer to G. Finocchiaro (edited by), *Right to anonymity. Anonymity, name and personal identity*, in F. Galgano, *Trattato di diritto commerciale e diritto pubblico dell'economia,* XLVIII, Cedam, Padua, 2008.
[54] Thus Rodotà, then President of the Guarantor Authority for the Protection of Personal Data, on the notion of the «electronic body», in the 2002 Report on the activity of the Data Protection Authority, Rome, Presidency of the Council of Ministers, 20 May 2003; ID., Technologies and rights, Bologna, 1995.

In addition, more detailed EU data protection rules have been adopted, but the right to protection of personal data was not finally guaranteed in the European Union as a "fundamental right of freedom" until December 1, 2009, with the entry into force of the Lisbon Treaty.

Article 6 of the Treaty on European Union (TUE) recognizes "the rights, freedoms and principles" politically proclaimed nine years earlier by the Charter of Fundamental Rights of the European Union (hereinafter Charter), adapted in Strasbourg, and the content of the European Convention on Human Rights. In addition, Article 52 of the Charter provides that restrictions may be imposed on the exercise of rights such as those referred to in Articles 7 and 8, provided that such restrictions are provided for by law, respect the essence of those rights and freedoms and are by the principle of proportionality[55]. Title II of the Charter of Fundamental Rights codifies the right to liberty and security (Article 6), respect for private and family life (Article 7) and the right to the protection of personal data (Article 8).

The Lisbon Treaty, as previously mentioned, had an enormous impact on the development of EU data protection regulations. The Charter was given the same legal value as the Treaties in Article 6[56] of the Treaty on the European Union. It, therefore, became a listed instrument, not only for the EU institutions and bodies but also for the Member States acting within the compass of EU law. The right to the protection of personal data was also specifically mentioned in Article 16 of the Convention on the functioning of the European Union among the general principles of the EU. The latter now provides a general legal base for the relinquishment of rules by the European Parliament and the Council, acting in the normal legislative procedure “relating to the protection of individuals about the protection of particular data” by EU institutions and bodies and by the member state acting within the compass of EU law, and “the free movement of similar data”.

[55] Article 52, Charter of fundamental rights of the European Union, TITLE VII, *Scope and interpretation of rights and principles*.
[56] Article 6, The Treaty on European Union (TUE), *The Rights, Freedoms and Principles.*

### 2.1.1. The Right of Data Protection

As provided for in EU legislation, the European Parliament and the Council recognize the protection of personal data as a fundamental freedom and repeal Directive 95/46/EC with Regulation 2016/679/EU thanks to Article 16 paragraph 2 of the Treaty on the Functioning of the European Union (TFEU).

In this legal framework, the protection of individuals regarding the processing of personal data means that great efforts are made to allow data processing based on the consent of the data subject or on another legitimate basis, and to create a strong set of rights to ensure each individual real "control over their own personal data"[57].

The European Union data protection model recognizes the "data subject" as having positive freedom of control and interference. The recognition of such far-reaching control and intervention protection for personal data suggests to the Italian authors that "data subjects" should not be considered passive subjects suffering from data processing, but rather as active entities defining their own identity.

According to Regulation 2016/679/EU, the right to the protection of personal data is more protected than in Directive 95/46/EC. In Chapter II, personal data are processed lawfully (if they meet certain applications such as the data subject's consent or other legitimate basis established by law or the legitimate interests pursued by the controller), fairly and transparently; the data are collected for specified, explicit and legitimate purposes (Articles 5-6-7). In addition, controllers must conduct an analysis and risk assessment to determine the appropriate measures (physical, logical, and organizational) to ensure the integrity and security of the data, which are adequate, relevant and limited, accurate and with a storage limit (Article 5-6-7).

The “data minimisation” principle is particularly relevant in GDPR since digital transformation and data exchange have evolved making frequent data collection for a variety of treatments.

---

[57] See recital 1, the General Data Protection Regulation, *Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.*

Regarding this set of rights, it is possible to point out that Regulation 2016/679/EU confirms with a great continuity Directive 95/46/EC, strengthening "data subjects' freedom": the right to live without arbitrary and unwarranted interference, intrusion, or limitation.

Considering the great technological evolution, the relevant perspective change in personal data protection is that the adequacy of measures adopted to protect the rights of a data subject must also be continuously tested and evaluated (the so-called "risk-based approach*"* Article 32 Regulation 2016/679/EU[58]). As the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default is affirming: "The GDPR adopts a coherent risk-based approach throughout its provisions, in Articles 24,25,32 and 35 with a view to identifying appropriate technical and organizational measures to protect individuals, their personal data and comply with the requirements of the GDPR. The risk and the assessment criteria are the same: the assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights and freedoms), considering the same conditions (nature, scope, context and purposes of processing)"[59].

In the next part of the Regulation, new tools are provided to guarantee each data subject what personal data can be processed to define "personal identity". Chapter III codifies the rights of data subjects to transparent information, communication and modalities for exercising their rights (Article 12); information and access to personal data (Articles 13-14-15 Regulation 2016/679/EU). These basic conditions protect the "human identity" and allow individuals to decide what kind of personal data can be processed thanks to the recognition of the rights to rectification, erasure, restriction of processing and the rights to data portability (Articles 16-17-18-19-20 Regulation 2016/679/EU).

This regulation also requires controllers to notify the "breach of security leading to the accidental or unlawful destruction or accidental loss of, alteration of, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" to the individuals whose personal data are affected (Article 4 and Article 34). The EU Independent Advisory Body on Data Protection and Privacy state that the new requirements strengthen the rights of data subjects because notifying them of a "data breach" allows them to "protect themselves against the possible consequences"[60].

---

[58] See WP29 Opinion 218/2014, *Statement on the role of a risk-based approach in data protection legal frameworks*.

[59]As the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, in: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

[60] See WP29, *Guidelines on Personal data breach notification under Regulation 2016/679*, 3 October 2017.

With this last set of rights, the GDPR maintains the previous protections, with a greater emphasis on the personal freedom of individuals. Under the new legal framework, data subjects can control and determine what personal data may be processed.

In addition, the right not to be subject to automated decision-making, including profiling, which has legal effects is strengthened in Articles 21-22 of GDPR. This was already provided for in Directive 95/46/ EC (Article 15).

According to the GDPR, data subjects have the right to obtain specific information on mathematical procedures, the right to have a human being intervene in the decision-making process, the right to express their opinion and obtain an explanation of the decision, and most importantly, the right to challenge and object to the decision (see Recital 71 and Article 22). Regarding the EU Independent Data Protection and Privacy Board, "human intervention is a key element. Any review must be conducted by someone with the appropriate authority and ability to change the decision. The reviewer should conduct a thorough assessment of all relevant data, including any additional information provided by the data subject"[61].

The authors emphasize that General Data Protection Regulation grants an important recognition that "it is obvious that an algorithm can only be explained if the trained model can be articulated and understood by a human. It is reasonable to assume that any reasonable explanation will include at least some indication of how the input features relate to the predictions". On the other hand, the right to explanation is said to be "a harmful constraint on artificial intelligence" because "it is often impractical or even possible to explain all decisions made by algorithms"[62].

The big question is how this language affects deep neural networks, which depend on huge amounts of data and generate complex algorithms that can be opaque even to those who use these systems. Algorithm-based predictive strategies could at the same time lead to a systematic violation of human dignity and the principle of non-discrimination that guarantees freedom of thought, choice, and action.

The analysis now moves to the important Chapter VI, which includes Articles 51 to 59, and concerns the "independent supervisory authorities" (Data Protection Authority, DPA), to which Article 28 of Directive 46 of 1995 was already devoted. In addition, this Chapter is divided into two sections: the first section concerns independence and includes Articles 51 to

[61] See WP29 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 3 October 2017.
[62] B. Goodman, S. Flaxman, *European Union regulation on algorithmic decision - making and a right to explanation,* AI Magazine, New York, Vol 38, No 3, 2017.

54; the second one instead concerns competence, tasks and powers, and includes Articles 55 to 59.

The first section is devoted to the definition of "supervisory authority" (Art. 51), the "conditions of independence" (Art. 52), the "appointment of members" (Art. 53) and the "rules on the establishment of the supervisory authority" (Art. 54). The main article of this section is therefore 51, which states that[63]:

- Each Member State shall provide that one or more independent public authorities shall be responsible for monitoring the application of this Regulation in order to protect the fundamental rights and freedoms of natural persons about the processing and to facilitate the free movement of personal data within the Union ("the supervisory authority").
- Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For this purpose, the supervisory authorities shall cooperate with each other and with the Commission, in accordance with Chapter VII.
- Where several supervisory authorities are established in a Member State, That Member State shall designate the supervisory authority representing those authorities in the Committee and establish the mechanism by which the other authorities comply with the rules on the consistency mechanism referred to in Article 63. [...]

The article just cited does not need further study, given its clarity and analytical, as indeed the following article, 52, which provides for the "conditions of independence". Section 1 concludes with the provisions on the appointment of members and the establishment of the Authority, as mentioned above.

In the second section describing the competence (art. 55), the tasks (art. 57) and the powers (art. 58) of the supervisory authorities, interesting innovations are represented by the figure of the leading authority (art. 56) and the territorial criterion for its competence. Article 55 opens Section 2 of this Chapter and speaks of competence as follows:

- Each supervisory authority shall be competent to carry out the tasks assigned to it and to exercise the powers conferred on it under this Regulation in the territory of its Member State.

[63] Article 51 of GDPR, *Supervisory authorities*, https://gdpr-info.eu/art-51-gdpr/.

- Where the processing is carried out by public authorities or private bodies acting based on Article 6 paragraph 1 c) or e), the supervisory authority of the Member State concerned shall be competent. In that case, Article 56 shall not apply.
- The supervisory authorities shall not be competent to supervise the processing carried out by the courts in the exercise of their judicial functions.

Before analysing the figure of the lead authority provided for in Article 56, however, it is appropriate to make a small reference to the provisions of Articles 57 and 58.

Article 57 sets out a very wide range of tasks for a supervisory authority on its territory, including the duty to: monitor the correct application of the Regulation (lit. a); promote knowledge, awareness and understanding of the risks, dynamics and safeguards related to protection personal data (lett. b); to advise parliaments, governments or national institutions (lett. c); promote the awareness of controllers of their obligations and duties (lit. d); dealing with complaints from a data subject (lit. f); cooperate with other authorities through the exchange of information (lit. g); performs any other task related to the protection of personal data (lit. v).

However, Rule 58 of the Rules of Procedure allows each authority to exercise three groups of powers:

- The first group shall consist of investigative powers, including the power to order the holder to provide him with all kinds of information, to allow him access to data and premises where necessary for the performance of his duties, or the possibility of carrying out investigations in the form of a data protection review, carrying out reviews of the certifications issued and finally notifying the holder and the controller of alleged infringements of regulatory provisions.
- The second group, on the other hand, is composed of corrective powers which are expressed in the power for the guaranteeing authority to issue warnings to the controller or processor when the processing may infringe or have infringed the provisions of the Regulation; order the data controller to comply with the data subject's requests to exercise his or her rights, to comply with the processing, to notify the data subject of the personal data breach, to temporarily or permanently limit the processing, to rectify or delete personal data, the suspension of data flows to a recipient in a third country.
- Finally, the third group provides for authorisation and advisory powers where the authority is required to: advise the holder in accordance with the prior consultation

procedure, deliver opinions to parliaments, governments, other national bodies and institutions and the public on matters relating to the protection of personal data; issuing certificates and approving their criteria; adopting standard data protection clauses; and finally approving binding corporate rules.

In conclusion, paragraph 4 provides for the general principle whereby the exercise of the powers of a supervisory authority is subject to appropriate safeguards such as the possibility of effective judicial review and due process, whereas, in paragraph 5, it is stipulated that each Member State must have the power by law for the supervisory authority to bring a judicial or extrajudicial action if the Regulation is infringed.

## 2.2. Regulations and Provisions of the GDPR

The main objectives to pursue in the elaboration of the EU Regulation 2016/679, from the European Legislator point of view, can be described by the creation of a framework of greater legal certainty and greater uniformity of the privacy rules in the various European countries, the identification of a legal basis for processing, the improvement of data protection of data subjects, but above all the responsibility of the data controller.

### 2.2.1. Some definitions

Article 4 of the General Data Protection Regulation contains a series of definitions that help the reader to understand the other provisions in the employment relationship more easily.

First, a definition of “personal data” is given, that is, any information concerning an identified or identifiable natural person. It is understood that the Legislator, with “any information”, recalls objective but also subjective data, such as opinions and valuations.

With reference to the concept of identifiability, a person is considered identifiable who can be directly or indirectly identified following a particular reference, such as name, IP of PC,

cookies, etc. Recitals 2 and 27 of the Regulation exclude from the object of the processing the data of deceased persons or anonymous data.

The definition of "sensitive data" under Directive 95/46/EC changes. They are now referred to as "special categories of personal data" pursuant to article 9 of GDPR; in particular, data relating to racial or ethnic origin political opinions and religious or philosophical beliefs, trade union membership, health data, genetic data, biometric data fall into this category, data relating to a person's sexual life or sexual orientation. The Regulation prohibits the processing of this category of data, but provides for certain derogations from paragraph 2 of that Article, including the provision of explicit consent for one or more specific purposes of the data subject, the case of the processing necessary to fulfil obligations or exercise specific rights of the controller or the data subject in matters of labour law or social security, and social protection in case of processing for purposes of medical assessment objective of the employee.

Article 10 states the processing of "Judicial Data" or relating to criminal convictions and offences: the processing must take place under the control of the public authority or subject to authorization by EU or Member State Law.

The Regulation introduces many definitions missing in the Italian Privacy Code. We refer to the definition of "archive", partly coinciding with "database": in the Regulation we speak of "structured whole", while in the Italian code we speak of "organised complex". The issue is of considerable importance, as the Regulation of article 2 indicates that in addition to all automated processing, the discipline also applies to non-automated processing, but only if data is present, or intended to be, in the archive.

Moreover, the Regulation specifies the definitions of profiling, limitation of processing and pseudonymization: the first is defined as automated data processing that produces assessments on certain personal aspects of the data subject; with the second we mean the marking of personal data stored with the aim of limiting their future processing; while the third definition indicates the mechanism of retention of data that cannot be attributed to a specific date subject without the use of other information that is stored separately.

What is meant by data processing and who is involved in the operations? Article 4 paragraph 2 contains a specific definition: "Any operation or set of operations, carried out with or without the aid of automated processes and applied to personal data or sets of personal data, such as collection, registration, organisation, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, comparison or interconnection, limitation, cancellation or destruction". The natural or legal person that determines the purposes and means of processing is defined in

art.4 paragraph 7 as "data controller"; note the presence of another category of subjects, defined "data processors" (indicated by art.28) or the persons in charge of data processing on behalf of the data controller.

The strategic point that makes it possible to clearly identify the distinction between the first category and the second is the identification of the subject that determines the purposes and means of treatment. Note absolutely the recommendations of the GDPR in the appointment of the data processor: it is necessary, first, the processing the act of appointment signed by both parties but, above all, the characteristic of "GDPR compliant" of the controller. The authorization must indicate, inter alia, the security measures taken by the person responsible.

The "minimum" security measures that every "dealing" subject must adopt are indicated in Article 32 of the Regulation, paragraphs a) to d):

- Pseudonymization and encryption of personal data.
- Ability to ensure the confidentiality, integrity, availability, and resilience of systems and processing services.
- Ability to restore the availability of access to personal data in a timely manner in case of physical or technical accidents.
- Establishment of a procedure for testing and evaluating the effectiveness of technical measures; and to ensure the security of processing.

The holders of the same treatment can be multiple (if they jointly define purposes and means): the situation is regulated by Art. 26 of the Regulation that deals with the category of the "joint data controllers". The provisions that apply are the same as those of the data controller but there is provision for the conclusion of an internal agreement between the parties indicating their respective positions, functions, and responsibilities in the fulfilment of obligations arising from the regulation.

The Regulation lacks a precise definition of "in charge" (present instead in the Italian Code), but it refers to it, within the definition of "third party", as a "person authorised to process data under the direct authority of the owner or manager". There is no obligation to nominate the person “in charge” but there is instead an obligation to train and to keep the reserve.

### 2.2.2. General Provisions and Basic Principles

The Regulations begin with some general rules, divided into two chapters: the general provisions themselves and the principles. The general provisions (Articles 1 to 4) are intended to identify the subject matter, the aims, the definitions (already developed in the previous paragraph) and the territorial scope.

With reference to the latter, art. 3 lays down the limits of the effectiveness of the rules: the criteria to be respected concern the residence of the data processor and certain special cases. The first criterion provides for the application to processing carried out by entities established in the European Union (regardless of whether the processing is carried out or not in the Union); the second criterion, on the other hand, provides for the taxation of those who although they are not located in the European Union, they process personal data according to the cases strictly provided for in the article, which is the supply of goods or the provision of services to data subjects established in the EU and the monitoring of data subjects within the EU.

Chapter II of the Regulation indicates the principles to be respected, the first step towards the status of "GDPR Compliant". Among the most important are the principle of legality, fairness and transparency; nevertheless, the principle of accountability, an absolute novelty of the Regulation, and the minimization of data.

Processing is lawful only if it takes place in compliance with the law. The processing of data depends on the occurrence of one of the situations indicated in Article 6 of the Regulation. It is possible to divide the processing into two macro-categories: the case in which the data subject has given consent (required in all data processing pursuant to Art. 9, with specific purposes) and where the data subject has not given his consent, but the processing is necessary:

- the person has given his or her consent to the processing for specific purposes,
- processing is necessary for the performance of a contract to which the person concerned is a party,
- processing is necessary for fulfilling a legal obligation,
- processing is necessary to protect the vital interests of the data subject or of another natural person,
- processing is necessary for the performance of a task carried out in the public interest or I the exercise of official authority vested in the controller,

- processing is necessary to pursue the legitimate interest of the controller or third parties, provided that no overriding interests or fundamental rights and freedoms[64].

In the first case, the burden of proof rests on the controller: it is his task to draw up a clear and easily understandable written declaration for the data subject, which must be signed freely.

In the second case, we have listed all the conditions for which data can be processed without having consent from the data subject. These conditions will be better analysed in the next part of this analysis.

The obligation of "accountability" is integrated by the GDPR, as a principle which requires that organisations put in place appropriate technical and organisational measures in order to be able to demonstrate what they did and its effectiveness if requested.

New disruption of the Regulation involves the full responsibility of the data controller regarding the methods, security measures and limits adopted. Before 25 May 2018, art.17 of the Privacy Code was in force, which maintained that the processing, excluding sensitive data, had to follow the measures and measures taken by the Guarantor (including the preliminary verification or the direct request for the opinion of the body); with the new regulation there is no longer the obligation of prior verification but the data controller must assess the compliance and adequacy of the processing and must always be able to prove that it is not in breach.

Another principle is linked to the "minimization of data processing": the data processed must be indispensable for the purpose of the data controller and any other superfluous and/or unnecessary data must be obscured or otherwise deleted from processing.
The data shall be accurate and updated as necessary. They must also be kept for a period of time not exceeding the achievement of the purpose for which they are treated, and the provision of a protection system is necessary to keep them intact and protected.

[64] Art.6 EU Regulation 2016/679, paragraphs a) to f), *Lawfulness of Processing*.

### 2.2.3. The Rights of the Data Subject

The data subject's rights are dealt with in Chapter III of the General Data Protection Regulation; the opening article stresses the duty of the controller to take appropriate measures to provide the data subject with all the necessary information in accordance with the key principles on which the rules are based.

First, the data subject has the right to know the purposes of the processing and the rights exercisable by him, the contact data of the data controller and the data processor, the retention period (or the criteria used to determine it), the categories of data processed, the existence of automated profiling processes, any third-party recipients of data and any legitimate interests of the data controller. The data controller is obliged to provide this information free of charge and without justified delay through the information (the maximum time is one month after receipt of the request, increased to two months in particular cases; in the case of data collection at the person concerned, as at the stage of establishment of the employment relationship, this must be informed at the same time as the transaction). Greater attention is given above all to the definition of "legitimate interest", however, underlined by Recital 47 of the Regulation and analysed thoroughly, with the prediction of recurring cases, by the Working Party (Working Group) ex-art. 2922 in elaborated No 249/2017.

The employer's main legitimate interest concerns the pursuit of entrepreneurial objectives and the protection of the company's assets, but this should not override the rights and freedoms of the employee (note that this also complies with the rules of the Workers' Statute). It is the task of the employer to assess in advance whether the processing of data is proportionate and justified to the pursuit of the legitimate interest (c.d. balancing test).

The last paragraph of Art. 13 provides that, in the event that the interested party is already aware of the mandatory information, then it is not necessary to deliver the information.

Articles 16 to 21 of the GDPR deal with other exercisable rights of the data subject:

- The right of access, or the right to obtain at any time from the controller confirmation that data is being processed or not and, if so, to receive a set of the information listed in Article 15 (purpose, recipients, profiling...). This provision indirectly imposes an obligation on the data controller to set up a system that allows all the information requested to be collected quickly and a copy to be delivered to the data subject (Recital

63 of the Regulation suggests the use of platforms from which the data subject can access remotely).

- The right of rectification, or the timely correction or modification of the data once the data subject has communicated it.
- The right to be forgotten (another novelty of the Regulation), or the right to obtain the rapid deletion of personal data in cases of withdrawal of consent, unlawful processing of data, completion of the purpose, and other cases. The right to be forgotten cannot be exercised if the processing is, among other cases, mandatory for the fulfilment of a legal obligation; it is understood that the employee, at least for the data necessary to the employer for the processing of the normal obligations, cannot require its cancellation.
- The right to restriction of processing in the event of the inaccuracy of the data processed or unlawful processing.
- The right to data portability, or the right to receive from the data controller a format containing all the personal data of the data subject that the data controller must transfer to another data controller (for example, the transfer of assignments from the previous employment consultant to the new one); this right is exercisable in cases where the processing is based on consent or a contract. Also, in this case, it is understood the need of the employer or in general of any holder, to develop a system that makes possible the creation of the "structured format".
- The right to object, which may be exercised at any time. The data controller must immediately stop processing the data unless it proves the existence of legitimate reasons that override the rights of the data subject.

It is easy to understand how the data controller is subject to a regulation for some very "risky" sides and it is clear the need to use all the necessary tools to adapt to the discipline.

With regard to remote controls, the data collected through video terminals must necessarily comply with the principles of the GDPR, while the lawfulness of the control deriving from the tools of the work rests, in addition to the adequacy of discipline and respect for privacy, also on the compliance of the information provided to employees. The information must specify the procedures for carrying out checks and data collection, otherwise, the data collected will be unusable, including for disciplinary purposes. This topic will be analysed in more detail in the last chapter.

### 2.2.4. Other Requirements: The Register of Processing, the DPIA, the Appointment of the DPO

The Regulation prescribes a series of obligations that must be carried out in the event that the processing of data falls within the cases provided.

First of all is the "Data Protection Impact Assessment" (DPIA) indicated in art.35. The prior processing of the document is mandatory in three specific cases or the automated processing of data, including profiling, which produces legal effects on data subjects, large-scale processing of categories of data and large-scale systematic monitoring of a publicly accessible area. Looking more closely at the case studies, one might think that impact assessment is mandatory only for a restricted target of data controllers. The first case is very rare, the second and the third case are based on the concept of "large scale".

According to Recital 91, the large-scale concept concerns a substantial processing of the quantity of data which must be measured by identifying the quantity of direct data subjects in relation to the number of data subjects combined by the same or the same characteristic geographical scope, affected by the same purpose of data processing. In fact, the art. 35 of GDPR[65] opens by expressly stating that the processing of data must be anticipated by the impact assessment "whenever it represents a high risk for the rights and freedoms of natural persons": the link to the principle of accountability is clearly established and the obligation for most data handlers to develop evaluation. The obligation of the DPIA is, according to the Guidelines of the document Working Party 29 n.24824, in some cases specifically indicated; among the mentioned are the case of processing of sensitive data and continuous monitoring of employees through video surveillance systems.

The DPIA must contain at least a systematic description of the processing envisaged and the purposes of the processing, including any legitimate interests; it must also contain an assessment of the necessity and proportionality of the processing according to the purposes, the risks to which the data processed are subject, the security measures put in place by the data controller and any residual risks that cannot be eliminated. The peculiarity of the impact assessment lies in paragraph 11 of art.35 which prescribes the obligation to revise the document at least when changes occur: it is a process of continuous review, not a single simultaneous fulfilment at the beginning of the processing and, in particular, in the event that the data

[65] Art. 35, GDPR, *Data Protection Impact Assesment.*

controller does not review the assessment, could be accused of not having assessed the risks and adopted security measures in accordance with the principle of accountability. It is available on the website of the Italian Data Protection Authority a software for the elaboration of a "standardised" impact assessment.

In the event that the impact assessment shows a high risk for the rights and freedoms of data subjects, not limited by security measures, the data controller is obliged to request prior consultation with the Privacy Supervisor; the request is subject to the ability of the holder to understand, through the reflections and evaluations previously carried out, the need for prior consultation.

The impact assessment clearly implements one of the cornerstones of the GDPR, the "privacy by design" or data protection from the moment of design, when the owner must make use of appropriate technical and organisational measures (such as pseudonymisation, minimisation, etc.).

As the Guidelines of 4 October 2017 clarify, although there is no general obligation to publish the DPIA, this is nevertheless recommended as a demonstration of the transparency and accountability adopted by the data controller. The register of processing is a further fulfilment required by the Regulation in Art. 30. It consists of a register containing all processing activities; the necessary information concerns the names and contact details of the data controller, the joint data controller, the controller and the data protection officer, rather than the purposes of the processing, the description of the categories of data subjects and categories of personal data, the recipients, the security measures are taken. The register must be kept in writing or in electronic format and must be communicated to the supervisor authority in case of prior consultation or if requested by the DPA.

Paragraph 5 of the article establishes the obligation of the register of the treatments for companies with more than 250 dependents, for the not occasional treatment of data ex art.9 and 10 and in general for every treatment that "may present a risk to the rights and freedoms of the data subject". This is the case for the recurring scheme, which is also valid for the impact assessment: at first, you feel that compliance is mandatory only for large, structured realities but from a more in-depth analysis the obligation for all those who process personal data derives.

In support of this thesis, the Annual Report of the European Data Protection Supervisor[66] has set out some recommendations on its website expressly indicating that the DPIA is not a

[66] Data Protection Supervisor (2018), *Guide to the application of the European Regulation on the protection of personal data*, Luxemburg, Edition update February 2018, p.26-27, in: https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf.

formal obligation but an integral part of the system of proper management of personal data and inviting the processing and the persons responsible, regardless of the size of the organisation or business, to take all the necessary steps to draw up such a register.

The new figure is that of the DPO, Data Protection Officer. The designation of a manager, external or internal to the company, is the responsibility of the data controller and is provided, also in this case, to the occurrence of situations expressly indicated in the Regulation. The designation is mandatory for data processing by public entities with one exception (the Court in the exercise of its functions) and for all those private entities that carry out main activities of regular and systematic monitoring of data subjects or processing of sensitive and/or judicial data (including data relating to health and union membership) on a large scale; the case histories are alternative. It falls on the concepts already seen in the field of impact assessment.

The opinion of the Working Party n.243/2016[67] assists with more precise ways in the interpretation of these concepts as a little "volatile", typical of the phenomenon of "soft law", argues in particular that the large-scale concept should be measured as the number of subjects affected by treatment, in absolute terms or expressed as a percentage of the reference population, the volume of data and/or the different types of data subject to processing, the duration, or the persistence of the processing activity or the geographical scope of the processing activity and provides several examples. On the other hand, the concept of regular and systematic monitoring, which is certainly relevant for remote controls, is understood as the monitoring of the behaviour of those concerned, which takes place at defined intervals or at least repeated over time according to a time pattern, implemented through a predetermined system or implemented as part of a strategy. Redirection of email messages, profiling and scoring activities for risk assessment purposes (for example, for fraud prevention and thus for "protection of corporate assets"), and location tracking, for example by mobile apps or video surveillance systems are examples expressed and dealt with in the above document.

The role of the Data Protection Officer encompasses all issues relating to data processing, from advice to employee training, from monitoring GDPR compliance to impact assessment advice rather than cooperation with the supervisory authority. He must be provided with all the means necessary for the performance of his duties and he must not receive any indication from the controller/processor concerning the performance of his duties. It is directly

[67] Article 29, Data Protection WP, *Guideline on Data Protection Officer, in:* https://ec.europa.eu/newsroom/article29/items/612048/en.

responsible together with the controller and processor and cannot operate in the event of a conflict of interest.

The figure of the DPO is subject to the requirements of professionalism and specialist knowledge in the field of privacy; again, the Regulation does not provide a precise list of specific requirements but is limited to indicating the skills in a general way. The legitimacy of the action lies in the request for communication of the name presented to the DPO for the protection of personal data through an online procedure. The designation of the DPO may also be voluntary, at the discretion of the data controller, following the assessments made by him. If the DPO is designated voluntarily, the same rules as in the case of compulsory designation obviously apply. However, EU or Member State law may provide for other mandatory cases, in addition to those of the Regulation.

## 2.3. The Evolution of Data Protection in the Employment Relationship

The problem of the protection of privacy in working relationships, and in the multiform manifestations of the use of information technology, is part of an ever more complex sector system, both for the technical content of the provisions and for the plurality of sources that characterise it. This sectorial order reflects not only the aspiration and concern of individuals, who intend to defend the privacy of their acts and the intimacy of their private life from the intrusive manifestations of others but also those who want to keep safe their identity and freedom of political decision.

Today, more than a century later, the right to privacy, understood as the founding value of individuality and recognition of the power to act as the owner of his data, even though it has become a universal right of the person, must deal with the socio-economic evolution of society and with the profound transformations due to the incessant technological progress of the forms of mass communication. In this context, a new and different concept of privacy is elaborated as new classifications in the knowledge that technical-scientific progress opens completely new perspectives, of which the conceptual schemes and the defence techniques previously elaborated are completely inadequate.

The problem of the use of new information and telematic technologies also takes on implications in the context of working relationships where the provisions dedicated to this problem are not limited to the regulation of data management and circulation through special guarantees but also reflect the speciality of the contractual link. In this last case, the direct involvement of the person poses the problem not only of the management of personal data but also of the limits to the control of the way in which work is carried out, on the behaviours kept in the company, where the contact with information technology and other technologically advanced work tools allows for privacy interference and control sometimes penetrating the opinions and manifestations of life outside work[68].

The personality of fulfilment is, moreover, the necessary precondition for subordination, the content of which affects the subjective sphere of the worker precisely because he is obliged to carry out himself, employed and under the direction of the entrepreneur, certain useful conduct[69]. And since the implementation of such conduct must be functional to the interests of the employer, the performance of work presupposes a constant commitment of coordinated cooperation by the creditor, who is recognized as having the functional power to organise, determine and direct the activity of others.

Therefore, the personality of the performance, subordination and organisational powers of the employer, while representing conceptually distinct profiles, are closely related to each other: the employee personally engages in the fulfilment of the obligation to work; subordination is determined by the specific work performance because it is dictated by the technical and functional needs of the organisation; the employer can carry out his activity in the most suitable ways to make it useful and profitable in the interests of the company, organising capital and labour.

In this context, the fulfilment of the obligation to work is divided into a series of behavioural obligations coordinated by the employer, in respect of which positions of supremacy and subjection are determined and in which a complex of instrumental legal situations that you carry out surveillance activities in order to satisfy the particular interests of the organiser: with the consequence that the rights to guarantee human dignity, to which the right to privacy belongs, should be distinguished; duties of non-interference by third parties so that the interest of the owner is satisfied.

---

[68] A. Bellavista, *Il controllo sui lavoratori,* Turin, 1995.
[69] M. Grandi, *Rapporto di lavoro*, in Enc. Dir., vol. XXXVIII, Giuffrè, Milan, 1987.

In fact, in this direction and in terms of regulatory techniques, the regulation of the Workers' Statute, with provision for a procedure union and administrative authorization of the control of workers in the company, reflects the evolution of the mandatory functional norm to the choice of limiting the technocratic ideology placed at the base of productive activities. Thus, the protection of dignity and confidentiality of workers is transformed from an instrument of provision of universal and abstract protections, informed by the logic of a rigid legal guarantee, in a union and administrative control, through a regulation that allows adapting the protections to protect workers to the needs of the concrete situation, considering an education and a position of contractual imbalance and a need for equal treatment of all workers.

As for the object of protection, there is no doubt that the right to privacy, as a fundamental right, is in short, the right to retain the possession of self and of their own identity. However, while the civil doctrine has lingered on the structure of the rights of the personality, united by the relevance to non-economic interests and considered to protect the personal sphere of the individual; labour law also imposed their dimension and about their antagonistic role, precisely because of the link between the technical aspects of the productive organisation and the relations of power-duty inherent in it.

### 2.3.1. General Legal Framework on Data Protection

The possible interactions between the protection of privacy and the control of workers have been one of the most debated topics for all actors in the legal world until today. This, at least in Italy, probably has a very specific reason: a new legal framework has been created in this area, both for the much-discussed modification of the rules for the remote control of the employer's work and for the new European legislation on the protection of personal data, Regulation (EU) No. 2016/679 (GDPR). The first was implemented in September 2015 by one of the four decrees implementing the Jobs Act[70] of 2015, Art. 4 of the Workers' Statute[71].

[70] Decretal legislative 14 September 2015, n. 151 (in Suppl. Ordinary n. 53 alla G. U., 23 September 2015, n. 221). Provisions for the rationalisation and simplification of procedures and obligations on citizens and undertakings and other provisions relating to the work and equal opportunities, in implementation of the law 10 December 2014, n. 183.
[71] Act No. 300 of 20 May 1970 (in G. U., 27 May 1970, No. 131).

We could say that a common point underlies the innovations in the discipline of distance control in the field of work and privacy as already anticipated: the need to face new challenges, developments, and technological changes of our time that we are experiencing in a globalised world.

Currently, as previously anticipated, there is no specific legislation on the processing of personal data in the context of employment relationships. There are, however, several documents that deal directly or indirectly with this issue.

In 1997, the Commission addressed the issue in a communication[72], in which it reaffirmed the full applicability of the personal data protection directives to employment relationships. Several consultations followed, one in 2001[73], which was already a direct result of the Communication, a second in 2004[74], which was launched by the Commission itself. The most important contribution came from the Art. 29 Working Party[75], which organised several meetings and study sessions[76] on the subject during these years. However, despite many attempts, no European legislation on the uniform protection of personal data in employment relationships was adopted.

It can certainly be said that the interest in the protection of personal data in the context of employment relationships has matured, especially in recent years. In fact, under Directive 95/46/EC there were no specific rules for the processing of personal data of employees. Protection was reserved for anyone in possession of personal data used by others for commercial purposes and was limited to promoting the development of codes of conduct for the correct application of the general rules in the presence of sectoral specificities[77].

[72] Communication from the Commission, *The social and labour market Dimension of the Information Society*, People Fist-Next Steps, Brussels, 1997.
[73] Communication from the Commission, *First stage consultation of social partners on the protection of workers' personal data,* Brussels, 2001.
[74] Communication from the Commission, *Second stage consultation of social partners on the protection of workers' personal data,* Brussels, 2004.
[75] This is the Working Group for Article 29, established by Art. 29 of the Directive 95/46. The Working Party Art. 29 is an independent advisory body composed of a representative of the personal data protection authorities designated by each State by the EDPS (European Data Protection Supervisor), as well as by a representative of the Commission.
[76] Among the most relevant are the Working Group on Data Protection - Article 29, 5401/01/IT/def. WP 55, working document on the supervision of electronic communications at the workplace, adopted on 29 May 2002.
[77] Cf. Art. 27 of Directive 95/46/EC.

Another building block in this picture is the recommendation of the Committee of Ministers the Council of Europe of April 1, 2015, to member states[78], which aims to update the current legislation and adapt to the new media, to the new technologies that are now also common in labour relations, both in the public and private sectors. The Recommendation was adopted as part of the negotiations between the Council and the European Parliament on the Rules of Procedure.

On this occasion, the attention of the member states of the Council of Europe is drawn to the need to protect the personal data of workers in the various areas in which they are collected and processed (see, for example, data collected in connection with recruitment for the purpose of fulfilling legal obligations, or data collected for work purposes, including via ICT or video surveillance systems)[79].

In addition to reaffirming the general principles to be respected in the context of the processing of personal data, certainly in employment relationships, the specificity of the Recommendation is that it has developed specific rules for the remote monitoring of the employee's activity, both through computer surveillance and the use of tracking devices, which will be analysed more in details on the last chapter of this thesis[80].

However, a fundamental problem remains: the recommendations are ineffective and have no legal consequences. Their use, therefore, merely makes it possible to publicise the positions of the European institutions and to propose courses of action and direction in the hope of achieving a common policy.

In the Italian legal system, the limits of control of the employee's activity are redefined by the central importance of the law D.lgs. 196/2003, Code on the processing of personal data (also known as the Data Protection Act), which prescribes the need for a balance between the legislator's power of control and personal rights. In fact, it has been stated that "the processing of personal data shall be carried out with respect for fundamental rights and freedoms, in

[78] Recommendation CM/Rec. (2015) 5 of the Committee of Ministers to the Member States on *processing of personal data in the context of employment.* Adopted by the Committee of Ministers on 1 April 2015, during the 1224th meeting of the Ministers' representatives.
[79] Recommendation of the Council of Europe CM Rec (2015)5 e Jobs Act: *profili di compatibilità e prospettive di tutela,* in ADAPT Bulletin, March 26.
[80] The framework is presented in the second part of the Recommendation, details on types of treatment, from Art. 14 to Art. 21.

particular, but not exclusively, the right to confidentiality, personal identity and the protection of personal data"[81].

Article 4 of Law 300/1970 provides that information about the employee's work recorded in audio-visual documents, in log files related to the activity carried out by a computer, or in cookies related to surfing the Internet, may be collected, used for "all purposes of the relationship", and kept by the employer if the employee is adequately informed about the methods of use of the instruments and the implementation of the controls, in accordance with the provisions of Law 196/2003[82].

The inseparable link between the protection of personal data and the person in the employment relationship is also formally recognized in the new regulation after GDPR.

Therefore, the decision of the legislator was to provide, through D.lgs. 101/2018, to introduce art. 101, which adapts the Code on the protection of personal data (Legislative Decree 30 June 2003, n. 196) to the provisions of Regulation (EU) 2016/679[83]. The provision expressly refers to the provisions of art. 88 of the European Regulation, lubricated "Processing of data in the context of labour relations", to which we must therefore refer to understand the current rules for the processing of personal data in the context of labour relations.

#### 2.3.1.1. Before the GDPR: Privacy Code D.lgs. 196/2003

Before the GDPR, Directive 95/46/EC was the main legal instrument for the protection of individuals with regard to the processing of personal data, aimed at facilitating the free movement of information within the EU. Adopted on 24 October 1995, with the aim of harmonising the rules and facilitating the free movement of personal data within the European Union, Directive 95/46/EC committed the Member States to implement, through national

[81] On the definition of the right to the protection of personal data v. G. Finocchiaro, *Privacy e Protezione dei Dati Personali, Zanichelli*, Turin, 2014, 151-152.
[82] Cfr. art. 4 comma 3^, Stat, lav, as it has been edited by art. 23 d.lgs. 151/2015.
[83] D.Leg 10 August 2018, No.101. Full Article on Gazzetta Ufficiale: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true.

transposition laws, legislation ensuring a high and uniform level of protection of citizens' fundamental rights and freedoms.

Directive 95/46/EC "Protection of natural persons with regard to the processing of personal data, as well as the free movement of such data" has played a fundamental role in trade, because it has allowed the removal of borders within the European Union, helping to create the conditions for the realisation of the free flow of data at the heart of the European agenda, as a strategy for the creation of the Digital Single Market.

Apart from its intentions, the Directive has only partially achieved the objective of offering greater guarantees regarding the protection of personal data, partly because of the differences between national transposition laws, in Italy Law 675/1996, then replaced by D. Lgs. 196/2003, containing the "Code on the protection of personal data", partly because of the purely commercial, which was accompanied by a bureaucratic conception of data management, information and consent of the data subject. The Italian legislator has harmonised the Privacy Code with the Regulation of the European Union by issuing Legislative Decree 101/2018 which amended and largely repealed, the provisions of Legislative Decree 196/2003.

The Italian Code D. Lgs. 196/2003 was a model of organic and comprehensive codification in the field of privacy. It consists of three parts: a) general provisions, concerning the substantive rules governing the processing of personal data, applicable to all processing, except for any specific rules for processing carried out by public and private entities; b) special provisions for specific processing operations, supplementing or excluding general provisions; c) provisions relating to the protection of the data subject and to the penalty system.

Article 3 introduced a fundamental principle, namely the “principle of necessity” in the processing of personal data, according to which: “Information systems and computer programs shall be configured by minimising the use of personal data and identifying data, so as to exclude their processing when the purposes pursued in individual cases can be achieved through, respectively, anonymous data or appropriate ways to identify the data subject only in case of need”. Following this principle, information systems and software had to be set up in such a way as to minimise the risk on personal data and could be used only if they were indispensable for legitimate and otherwise not feasible purposes.

For the rest, title VIII, of the d.lgs. n. 196/2003, dedicated to "treatments in the context of the employment relationship", contains a meagre discipline, essentially referring to other provisions. This latter contains six articles, all related to the processing of personal data in the employment context, which will be listed below.

- Article 111: focuses on the set of principles and rules of conduct to be observed in the employment context. “The Guarantor promotes, pursuant to article 2-quarter, the adoption of deontological rules for public and private subjects interested in the processing of personal data carried out under the employment relationship for the purposes referred to in article 88 of the Regulation, including specific arrangements for the information to be provided to the data subject.”
- Article 112:” Within the meaning of Articles 20 and 21, the objectives of establishing and managing public employment relationships of any kind, whether employed or self-employed, whether or not remunerated or honorary, or part-time or temporary, shall be deemed to be of significant public interest, and three forms of employment that do not involve the establishment of a relationship of subordinate work”.
- Article 113: “It remains without prejudice to the provisions of article 8 of Law 20 May 1970, n. 300”. Which states “It is forbidden for the employer, for the purpose of recruitment, as in the course of the employment relationship, to carry out investigations, including through third parties, on the political, religious or trade union opinions of the worker, as well as facts not relevant to the assessment of the worker’s occupational aptitude.”
- Article 114: “It remains without prejudice to the provisions of article 4 of Law 20 May 1970, n. 300”. Which defines: “The use of audio-visual equipment and other equipment for the purpose of remote monitoring of workers' activities is prohibited.”
- Article 115: “In the context of domestic and telework relations, the worker shall be required to ensure that his or her personality and moral freedom are respected. And the domestic worker shall maintain the necessary confidentiality with regard to all matters relating to family life”.
- Article 116: “For the performance of their activities, management and social assistance institutions, within the mandate conferred by the person concerned, have access to the data banks of the institutions providing benefits, in relation to data types specifically identified with the consent expressed pursuant to Article 23. Moreover, the Minister for Labour and Social Policy shall issue a decree with the Minister for Labour and Social Policy laying down the guidelines for special agreements to be concluded between the Welfare and Welfare Institutions and the institutions providing benefits”.

These articles state pretty clearly which rules were applied in the context of employment in 2003. As we will see in the following analysis, many articles will be reshaped or removed in accordance with the digital transformation environment that Industry 4.0 has enhanced. An important article that will be highlighted in the following thesis is number 114 of 196/2003, which corresponds to article 4 of Law 20 May 1970, n. 30. We will see how it could not be left unchanged given the working conditions that started to take place over the last years.

### 2.3.2. The GDPR in the Employment Context

As we have introduced in the previous chapter, the drastic technological changes, enhanced by the advent of the fourth industrial revolution, have completely overwhelmed the way to process data in the employment context. The adoption of new technological tools, infrastructures, applications and smart devices enables employers to collect and connect at any time and with an enormous number of employees' personal data. New types of systematic and potentially ever-present computing in the workplace, less visible than traditional surveillance cameras and more intrusive into private lives as employees work remotely, pose significant privacy and data protection challenges. This ongoing transformation involves the massive collection of employee data and the algorithms used for predictive functions in the company's decision-making process, a potentially huge transformation which has far-reaching consequences.

The rapid evolution of technology has contributed to increasing the perception of the risk of privacy breaches, and to spreading greater sensitivity towards the issue of data protection. As a consequence of this, in 2016 a new regulation has been introduced: General Data Protection Regulation (GDPR, 2016/679/EU)[84]. This latter has provided a harmonised, consistent, and comprehensive framework on the processing of personal data, to protect humans' privacy and dignity with regards to their data.

[84] Regulation EU no. 2016/679 (GDPR) e D. lgs. 30.06.2003.

In the employment context, however, the GDPR has enacted only Article 88[85] that explicitly focuses on the workers' data protection, leaving to the Member States the obligation to amend or replace their respective national data protection laws to align with the GDPR. Regardless of the great importance of individual rights in the employment context, the European Union has not already established harmonised rules.

Therefore, the concept of the protection of personal data is not considered an "absolute right" in the new EU legal framework since each Member State could provide more specific rules for this form of protection. Many multi-level legal frameworks apply to this right to the protection of personal data, such as CEDU, EU Treaties, Directives and Regulations. For this reason, it will be crucial to reassess the right of workers to the protection of personal data in order to avoid misunderstandings, inconsistencies, and confusion.

The protection of personal data, which was first codified as a right to respect for private life and then as a freedom and individual human right, is not protected by specific rules in the GDPR for workers. Workers' right to data protection is not given special protection in such a way that it takes precedence over companies' interest in improving their business through the processing of personal data. In the unified framework of the GDPR, there should always be a balance between the rights and interests of workers and businesses. This is evident from the guidelines on transparency under Regulation 2016/679, Article 29 Working Party, so-called "WP29"[86], which anticipate the future work of the European Data Protection Board (EDPB) by issuing guidelines, recommendations, and best practices to promote a consistent application of the GDPR (Article 70, Regulation 2016/679/EU[87]).

General Data Protection Regulation does not provide for specific uniform rules to protect workers throughout the EU, but at the same time, it allows each Member State to adopt specific rules to protect workers' right to personal data. In this important matter, we could have different national rules, but also the possibility to strengthen the protection of workers' personal data in each Member State: ensuring procedural rules thanks to Article 88 of Regulation 2016/679/EU.

[85] Article 88, EU GDPR, *Processing in the context of employment.*
[86] The Article 29 Working Party (Art. 29 WP) is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR).
[87] Article 70, EU GDPR, *Tasks of the Board.*

### 2.3.2.1. Recitals of the GDPR in the Field of Employment

The General Data Protection Regulations is composed of 99 articles and 177 recitals. These latter provide additional information and supporting context to supplement the articles.

The first recital that directly relates to the processing of personal data also in the area of labour law is Recital No. 52[88], which provides that exceptions to the prohibition on processing certain categories of personal data should also be allowed where provided for Union or Member State law. However, there is one clarification: the safeguards for the protection of personal data and the fundamental rights of individuals must always be respected. The recital immediately underlines the importance of the right to the protection of personal data and fundamental rights, which may only be sacrificed in exceptional cases. Derogation is possible, but only if the processing is in the public interest.

Explicit reference is made to the processing of personal data in the sector of labour law, provided that the aims are health-related, including public health and the management of health care services, and in particular in order to ensure the quality and cost-effectiveness of the procedures for satisfying requests for services and services under the health insurance scheme, or for archiving in the public interest or research.

The derogation, the recital concludes, should also allow the processing of such data, where necessary, to establish, exercise or defend a right in judicial, administrative, or out-of-court proceedings.

There seems to be a strict and very limited list of the purposes that would legitimise the processing, exceptionally, of this type of data. Recital 54[89] shows the rigidity of the derogations. It specifies how the processing of such data may be necessary for reasons of public interest in the field of public health[90] without the consent of the data subject. In the final part it is pointed out that the processing of health-related data, carried out for reasons of public interest, should not involve the processing of personal data for other purposes by third parties, among which the employers stand out.

[88] Cf. recital No. 52 of Regulation (EU) No. 2016/679.
[89] See recital 54 of Regulation (EU) No 2016/679.
[90] The Regulation specifies that the term 'public health' should be interpreted in accordance with the definition in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (G. U. L 354 of 31 December 2008, 70).

Recital 155[91] gives rise to considerable uncertainties and allows Member States or collective agreements, including company agreements, to lay down specific rules for the processing of personal data in the context of employment relationships. This applies, in particular, to the conditions under which such data may be processed on the basis of the employee's consent, for the purposes of recruitment, execution of the employment contract and all that follows from it.

The extent of discretion given to Member States in this area is clear, but the consequences of this are very worrying: lack of coherence, homogeneity, and harmonisation within the EU.

To close the circle and connect the recitals just mentioned, Art. 9[92], treatment of special categories of data, which provides for a general prohibition on the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or sex life or sexual orientation of the person concerned.

The second paragraph contains an extensive list of exemptions mentioned in paragraph 1. These include the processing of special categories of data relating to labour law, social security and social protection. This data may be processed insofar as the controller is authorised to do so by Union or Member State law or by a collective agreement under Member State law. This applies whenever there are adequate safeguards for the protection of the fundamental rights and interests of the individual.

Art. 9 ends with paragraph 4 above, "Member States may maintain or introduce additional conditions, including restrictions, for the processing of genetic data, biometric data or health data." The content of this paragraph is referred to in Recital 10[93] of the Regulation, which in turn provides "a margin of appreciation for Member States to determine their rules, including with regard to the processing of special categories of personal data ('sensitive data')". The Regulation also provides the possibility for Member States to determine their own rules. In this sense, this Regulation does not preclude the law of the Member States from determining the conditions for certain processing situations and also from determining more precisely the conditions under which the processing of personal data is lawful.

[91] See recital 155 of Regulation (EU) No 2016/679.
[92] See Article 9 of Regulation (EU) No 2016/679.
[93] See Recital 10 of Regulation (EU) 2016/679.

### 2.3.2.2. Article 88 of the GDPR

Art. 88 is the only provision that explicitly deals with the processing of personal data in the context of employment relationships. In order to make a detailed analysis of the norm, the text should be divided into several parts.

Paragraph 1 introduces an element of crucial importance. Indeed, it is based on the possibility for Member States to lay down more specific rules by law or collective agreement, including company agreements. These rules should aim to ensure the protection of rights and freedoms, for all purposes connected with the employment relationship.

The standard refers, in particular, to "the purposes of employment, the performance of the employment contract, including the fulfilment of legal or collective obligations, the management, planning and organisation of work, equality and diversity at work, health and safety at work, the protection of the employer's or client's property, and for the purposes of the individual or collective exercise and enjoyment of the rights and benefits connected with the work, and for the purposes of the termination of the employment relationship"[94].

Here, the discretion granted by the Member States to the social partners, who are explicitly given the possibility to have recourse to collective agreements, and company agreements, is clearly evident in the formulation and application of specific rules to protect workers' rights and freedoms. This is the same discretion referred to in Recital 155.

This margin for action gives rise to several concerns, but these are immediately mitigated by the overriding need to protect fundamental rights.

Indeed, the second paragraph provides that the rules referred to in paragraph 1 must include appropriate and specific measures to protect the human dignity, legitimate interests and fundamental rights of the data subjects. This passage expresses the will of the European legislator, who is trying to combine two conflicting interests: on the one hand, that of the employer and thus the efficiency of the company, and on the other hand, that of the employee, whose rights cannot simply be sacrificed.

[94] ILO (International Labour Organization), *Protection of Workers' Personal Data,* in: https://www.ilo.org/legacy/english/intserv/working-papers/wp062/index.html.

Of fundamental importance is the last part of the second paragraph, which states that the appropriate measures must relate in particular to the transparency of processing, the possibility of transferring personal data within a group of undertakings or a group of undertakings engaged in a joint economic activity, and control systems. On this provision, the European legislator's awareness and concern about technological change and the ever-changing problems associated with it peacefully emerge.

The direct and immediate consequence of the provision is that, in the context of industrial relations, as we become familiar with the new regulation, we will continue to be confronted with different data protection regimes specific to each Member State[95].

It must be stressed here that the regulation has a territorial scope "extra-EU", so all companies that have or want to have access to the European market need to know what impact it will have. This means that the new regulation will fully apply to companies, including those based outside the European Union, that provide services or products to people in the Union. All such companies, regardless of where they are based, will have to comply with the new rules, as will all companies that control employees based in the Union.

In addition, employers should be well aware that the Regulation will also apply to data processors[96], that is to say to any entity that processes personal data on behalf of the data controller, that is, the employer[97]. As an example, one of the questions that the employer will have to ask is which service provider it uses for human resource management and, if appropriate, will have to revise their contractual conditions to ensure that they comply with the Regulation. No matter where the service provider[98] is located.

Much emphasis is placed on the term "transparency" and on the information to be provided to the data subject; employers will have to inform employees, giving details of the legal basis

---

[95] A. Bevitt, C. Stack, *Preparing for the GDPR - advice for employers,* in Privacy and Data protection Journal (PDP), vol. 16, issue 6. Full article: https://www.cooley.com/~/media/cooley/pdf/reprints/preparingforthegdpr.ashx?la=en.

[96] Cf. Art. 4, EU Regulation n 2016/679, Definitions, n. 8 Data Processor, *the natural or legal person, the public authority, the service or other body that processes personal data on behalf of the data controller.*

[97] Cf. art. 4, EU Regulation n. 2016/679, Definitions, n. 7 Data Controller: *the natural or legal person, the public authority, the service or other body that, individually or together with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria applicable to its designation may be established by Union or Member State law.*

[98] Service provider is defined as *the entity that carries out an entrepreneurial activity as an information society service provider, offering connection, transmission and storage of data, or hosting a site on its equipment,* cf. Explanatory report to Legislative Decree no. 70/2003 on electronic commerce.

on which, the processing is carried out. An interesting recent Transparency Decree has been enacted in 2022 (analysed in the following paragraphs), which introduced some innovations regarding the processing of personal data of workers.

The recipients or any categories of recipients of personal data must be specifically identified, as must the period of storage of personal data, or, if it is not possible, will be indicated to the worker, the criteria used to determine that period. The data subject will be expressly granted the rights to ask the data controller for access to personal data, the rectification and cancellation of the same, the limitation of the processing concerning them or to oppose their processing, as well as the right to data portability and the right to withdraw consent. It should be noted that, among the rights, there is also the possibility for the data subject to lodge a complaint with a supervisory authority[99]. All such information should be presented in clear language, understandable and accessible.

In conclusion, employers must demonstrate that they have implemented an adequate, understandable, and effective data protection policy which provides employees with the information they need to process their data in accordance with the principles of transparency.

Article 88 concludes by stating that each Member State is obliged to notify the Commission of legal standards adopted under paragraph 1 by 25 May 2018, the date on which the Regulation must come into force. Subsequent changes to the national legislature must be notified immediately.

[99] Cf. art. 13, EU Regulation No. 2016/679, Information to be provided when personal data are collected from the data subject. With reference to art. 13, the new art. 111a of the Data Protection Act provides that, in the case of receiving resumes spontaneously transmitted by the data subjects for the purpose of entering an employment relationship, such information shall be provided to the first useful contact following the transmission of the resume itself.

## 2.4. Some Regulatory Sources from Data Protection Authorities

### 2.4.1. General Authorization No. 1/2016 of the Italian Data Protection Authority

In order to understand what the current regime of Italian law is regarding the processing of personal data of employees, it is appropriate to refer to a 2016 document of the Italian Data Protection Authority[100].

This authorization applies to all those who process sensitive data for the purpose of establishing, managing or terminating an employment relationship. The Decision recognizes that in many cases the process of sensitive data in the workplace may rely, as a legal basis, on the law and the employment contracts which justify the processing with respect to the fulfilment.

Specific obligations are imposed on employers before, during, and after the employment of data subjects. Before recruitment, confidential and general personal data may be processed only to the extent necessary for specific lawful purposes and to establish an employment relationship. Anything unnecessary for the establishment of an employment relationship should not be requested and should not be used even if provided. In this regard, for example, employers should not assume that they are permitted to process data contained in social networks for their own purposes simply because an individual's profile on social media is publicly available. In order to be able to carry out such processing, there must be a legal basis, such as legitimate interest, to ascertain, for example, whether the profile has a commercial purpose or was opened specifically to increase employment opportunities for employees[101]. Then without prejudice to the prohibition of the processing of employees' genetic data in the course of the employment relationship, this decision does not apply to (i) religious or philosophical beliefs or membership in associations or organisations of a religious or philosophical nature, and (ii) political opinions or trade union membership, or the exercise of public functions and political duties and provides for certain restrictions on the processing of data relating to trade union activities or duties.

[100] Authorization No. 1/2016, *Authorization to process sensitive data in employment relationships* of December 15, 2016 (published on G. U. No. 303 of December 29, 2016) [doc. web. n. 5800451].
[101] See, e.g., LinkedIn, Article 29 Working Party Opinion No. 2/ (see No. 2017).

This is the authorization for the processing of sensitive data in employment, which states that "[] in view of the fact that a large number of processing of sensitive data occurs in the context of employment relationships []" the Data Protection Authority " authorises the processing of sensitive data pursuant to Article 4, paragraph 1, letter d) of the Code, in accordance with the requirements set forth below []" [102]. The last point, temporal effectiveness, states that "this authorization shall be valid from January 1, 2017, to May 24, 2018, taking into account Regulation (EU) No. 2016/679 [] applicable as of May 25, 2018, without prejudice to any amendments that the Guarantor deems necessary due to new relevant legislation and without prejudice to any decisions issued by the Authority pursuant to this Regulation".

This is the status of 2016.

Today, the guarantor has made a very precise choice. With a decree of December 13, 2018[103] he has established the requirements of some general data authorizations from 2016, which are still in force with the regulation and D.lgs. 101/2018 to align them with the Data Protection Act. Of the nine existing authorizations, only five have passed the guarantor's review, including Measure No. 1/2016 on the processing of sensitive data in employment relationships.

This means that the processing of sensitive data of employees may only take place if it is aimed at managing employment relationships and if the methods described in the authorization are followed.

Before starting or continuing the processing, the information systems and computer programs must be configured to minimise the use of personal data and identification data. In this way, processing is excluded if the purposes pursued in the individual case can be fulfilled by anonymous data or other appropriate methods that allow identification of the data subject only if necessary.

Moreover, communications, including electronic communications, containing particular data, must be individualised; that is, the most appropriate measures must be taken to prevent the unjustified recognition of such data by persons other than the recipient.

[102] The document divides the requirements to be met as follows: 1) scope of application; 2) data subjects to whom the data relate; 3) purpose of processing; 4) categories of data; 5) modalities of processing; 6) conservation of data; 7) communication and dissemination of data; 8) Request for authorization; 9) Final provisions; 10) Temporal effectiveness.
[103] The regulation is no. 497 of December 13, 2018, doc. web n. 9068972.

The number of interested parties is very large and includes, in addition to employees, recruitment candidates, consultants and self-employed persons, agents, representatives and agents, self-employed persons, natural persons holding social positions or other positions in legal persons, bodies, associations and bodies, as well as third parties damaged in the exercise of the work or professional activity of the interested parties and their family members or partners for the issue of facilitations or permits.

In order to authorise the processing of sensitive data of employees, it is necessary that they are strictly necessary for the privileges, tasks or purposes provided for in the authorization itself and that they cannot be fulfilled or realised on a case-by-case basis through the processing of anonymous data or personal data of a different nature.

It follows that data controllers within the described scope of application are not obliged to apply to the guarantor for authorization if the processing complies with the requirements of authorization No. 1/2016[104].

### 2.4.2. The WP29 Opinion No. 2/2017

As previously mentioned, Regulation 2016/679/EU has not managed yet in regulating the employment context with uniform specific binding EU rules. GDPR has enacted only Article 88 that explicitly focuses on the workers' data protection. In this regard, it has been published in the Opinion 2/2017 over the article 29 of the Data Protection Working Party, which addresses specific points of the GDPR and, while not entirely up to date, is currently the most authoritative and comprehensive EU-level guidance.

It is important to analyse how the WP29 (Article 29 Working Party so-called WP29) defines the workers' risks to personal rights posed by the new ICT, and undertakes a general proportionality assessment, which consist of the balance of employees' rights and employers' legitimate expectation to process personal data in managing human resources.

[104] Cf. item 8) of measure No. 1/2016: applications for permits.

When considering employers, in Opinion 2/2017[105], it is highlighted that consent cannot licit data processing in the employment environment due to the nature of the labour relationship. As a matter of fact, pursuant to the particular data process, workers' agreement could hardly legitimate the personal data process, since the general reliance of the labour relationship infrequently puts workers in a position to freely give, resume or drop consent.

In opinion 2/2017, it is mentioned that in the majority of cases, the legitimate interest of companies could be invoked to process employees' data. And this latter will imply a proportional test, whether data is necessary or whether the processing over-cross the data protection rights and moreover, it is essential to perform an examination on which measures are required to ensure the right to private life and the right to secrecy of communications. When considering WP29, the processing purpose must be legitimate and the method proportional to the business needs: "Data Processing at work should be carried out in the least intrusive manner possible and be targeted to the specific area of risk". Some new requirements introduced by the GDPR are new security measures for data controllers[106], grant employees the right not to be subject to automated decisions[107], and prevent the most privacy-friendly solutions with data minimization[108].

Another important aspect to mention, related to GDPR, is the introduction to a Data Protection Impact Assessment (DPIA) if "a type of processing, in particular using new technologies, and taking into account the nature, scope and context and purpose of the processing itself is likely to result in a high risk to the rights and freedoms of natural persons"[109]. A data protection impact assessment is required whenever the processing may pose a high risk to the rights and freedoms of individuals. An impact assessment shall be required at least in the following three cases[110]:

- A systematic and comprehensive assessment of a person's personal aspects, including profiling.
- The processing of sensitive data on a large scale.

[105] Opinion 2/2017 on the processing of data in the workplace adopted on 8 June 2017.
[106] Article 17 Regulation 2016/679/EU, A*ppropriate technical and organisation measures*.
[107] Article 15 Regulation 2016/679/EU, *Right of Access by the data Subject.*
[108] Article 25 Regulation 2016/679/EU, *By design and by Default*.
[109] Article 35 Regulation 2016/679/EU, *Data Impact Assesment (DPO).*
[110] Important answer to the question *When a DPO on personal data is necessary?,* European Commission: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_it#:~:text=È%20necessaria%20una%20valutazione%20d,vasta%20scala%20degli%20spazi%20pubblici.

- Systematic and large-scale monitoring of public spaces.

Indeed, regarding recitals 71 and 91 of the Regulation 2016/679/EU, “results in high risk” evaluating or scoring, including profiling and predicting especially “aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements”. The impact assessment should be performed before treatment and should be considered as a live tool, not simply a one-time exercise. Where there are residual risks that cannot be mitigated by the measures put in place, the DPA shall be consulted prior to the start of processing.

#### 2.4.2.1 Risk Analysis and Proportionality Assessment proposed in the WP29 Opinion No. 2/2017

According to the establishment of the legal framework Regulation 2018/679/EU, WP29 proposes a risk analysis on employees’ data protection and proportionality assessment. In Opinion 2/2017, the independent EU Advisory Body analysed which situations, related to data processing in the employment context, could have potential damage to employee rights and moreover, focused on finding the balance between worker’s data protection rights and companies’ interests.

With reference to WP29, recruitment is the first personal data processing potentially damaging for workers. It refers to the use of social media extensively, and it is relatively common for user profiles to be publicly available depending on the settings chosen by the account owner. As a result, employers may believe that researching potential candidates' social profiles is justified in the hiring process. The same may be true for other publicly available information about potential employees. However, employers should not assume that simply because an individual's profile on social media is publicly available, they are permitted to process such data for their own purposes. Such processing must have a legal basis, such as legitimate interest.

In this context, before examining a candidate's social media profile, employers should first consider whether the profile is for commercial or private purposes, as this can be an important indicator of the legal eligibility of the examination of such data. Furthermore,

employers shall have the right to collect and process personal data on candidates only to the extent necessary and relevant for the performance of the job for which they have applied. As a general rule, data collected during the recruitment process should be deleted as soon as it becomes clear that there is no job offer or that the offer is not acceptable to the candidate. The latter should be appropriately informed of such treatment prior to the start of the recruitment process.

The risk analysis and assessment proposed are important since they point out that the "individual consent" during recruitment or in a general employment context could not be a lawful legal ground for data processing given the unbalanced relationship between the employee and the employer. In Opinion 2/2017, it is stated that in the employment context, the personal data process should be legitimate by legal grounds different from consent and in any case, should be proportionate, subsidiary, minimised and informed. Regarding WP29 the information on data processes should be communicated to workers whether companies process data publicly available or not.

The fair balance, between workers' data protection rights and companies' interests, stands on the protection of workers' right to "retain the option of a "non-work" non-public profile that they can use instead of the "official" employer-related profile, and this should be specified".

Another scenario in which processing the personal data of employees could be potentially damaging is concerned with the treatments resulting from screening during the period of employment. In view of the existence of social media profiles and the development of new analytical technologies, employers have (or may obtain) the technical capacity to carry out permanent employee screening, collecting, for example, information about their friends, opinions, beliefs, interests, movements, attitudes, and behaviour, thus acquiring data that also pertain to the private and family life of employees. Screening during the period of employment of employee profiles on social media should not take place on a generalised basis. In addition, the employer should refrain from asking an employee or candidate for access to information that they share with other people on social media.

Furthermore, employees should not be required to use a social media profile made available by their employer. Even if this is specifically provided for in view of the tasks entrusted to them (for example, acting as a spokesperson for an organisation), employees must retain the option of having a non-public profile, namely "non-working", which they can use in replacement of the "official" profile related to the employer, and this should be specified in the conditions of the employment contract.

The other scenario that could damage the processing of employees' personal data concerns the control of electronic communications in the workplace. Traditionally, monitoring electronic communications in the workplace has been considered the main threat to the privacy of employees. The conclusion in relation to the Working Document on the surveillance of electronic communications in 2001 remains valid, thus it is essential to consider all those technological developments which allow new ways of monitoring potentially more intrusive and pervasive.

Irrespective of the technology concerned or its capabilities, the legal basis referred to in Article 7 f) shall only be available if the processing meets certain conditions. First, employers using these products and applications should assess the proportionality of the measures they are implementing and whether further action can be taken to mitigate or reduce the scope and impact of data processing. As an example of good practice, such an assessment could be carried out through a data protection impact assessment before any monitoring technology is introduced. Secondly, employers must implement and communicate acceptable use policies, accompanied by privacy policies, describing the permitted use of the network and equipment of the organisation, and detailing the treatment in place. In some countries, the creation of such a policy would require the approval by law of the Council of Delegates or a similar body representing employees. In practice, such policies are often drawn up by staff in charge of maintaining computer equipment. Given that their main objective will therefore be safe and not the legitimate expectation of protection of employees' privacy, the Working Group recommends always involving a representative sample of employees in the assessment of the need for monitoring, as well as the logic and accessibility of the policy.

In some cases, employee monitoring is not enabled by specific technologies but simply requires employees to use online applications provided by employers that process personal data. Employees should be able to designate certain private spaces to which their employer does not have access, except in exceptional circumstances. For example, calendars are often used for private appointments. If an employee classifies an appointment as "private" or states so in the appointment details, the employer (and other employees) should not be able to examine the contents of the appointment.

In this context, the requirement of subsidiarity may also mean that monitoring is impossible. For example, it may be possible to prevent the use of prohibited communication services by blocking access to certain websites. If it is possible to block a website, one should choose to block it to meet the complementarity requirement instead of continuously monitoring all communications.

More generally, the emphasis should be on prevention rather than detection. Rather than expending resources to identify unauthorised use of the Internet, the interests of the user are better protected by preventing unauthorised use through technological means.

Another scenario that is important to be mentioned is related to the data processing operations resulting from monitoring ICT usage outside the workplace. This practice is becoming every day more common since the growth of home and remote working, due to the pandemic situation that our society has been through. Law has evolved in this matter by introducing the so-called "smart work" Act no. 81/2017, which allows employees to work anywhere outside the company. Nowadays, thanks to the rapid implementation of ICT equipment at home, it is almost possible to completely replace the workplace environment with the "home office".

Nevertheless, as Opinion 2/2017 has outlined, remote working presents additional risks for companies 'data security, since without the correct implementation of appropriate security tools to avoid risk, the risks of unauthorised access will drastically increase, inducing the loss or destruction of personal data of employees or customers for instance. There could be multiple suggestions to mitigate risks for data protection, such as allowing employers in logging keystrokes and mouse movements, screen capturing, enabling cameras, etc. On the contrary to this, Opinion 2/2017 focuses on the employer's possible lack of legal ground under legitimate interest for performing such monitoring activities (such as recording employees' screens).

The fair balance suggested in Opinion 2/2017 implies "addressing the risk posed by home and remote working in a proportionate, non-excessive manner" and, moreover, Opinion 2/2017 specifies that "monitoring the location and traffic of such devices may be considered to serve a legitimate interest to protect the personal data that the employer is responsible for as the data controller; however this may be unlawful where an employee's personal device is concerned if such monitoring also captures data relating to the employee's private and family life". Monitoring can also derive from Mobile Devices Management, which are tools that let the employer locate devices remotely.

Some suggestions are related to the implementation of highly sophisticated security devices, monitoring the traffic through a VPN, distinguishing private and business use of the device appropriate measures, and performing a Data Privacy Impact Assessment in order to value whether the resulting "data processing complies with the principles of proportionality and subsidiarity". Wearable devices are also very damaging tools for employers since they are able to process personal data related to health data and activities that happen outside the

workplace. In this regard, Article 9 Regulation 2016/679/EU entered into force by prohibiting the process of sensitive nature of data for employers since it is unlawful.

Another damage for employees could arise from the use of new tracking technologies, which allow a tract of employees' time and attendance and collect biometric data as well as mobile device tracking. In Opinion 2/2017, the processing could be necessary and lawful in the legitimate interests if the system complies with legal obligations to avoid unauthorised access.

The same concept applies when dealing with monitoring and surveillance by video or by technologies installed on company vehicles. In Opinion 2/2017, it is highlighted that each employer should avoid using facial recognition technologies or those tools that enable them to collect data remotely, to ensure a fair balance between employees.

Besides the basic GPS tracking systems, from telematics vehicles it is also possible to collect data not strictly related to the location but also related to the wealth of other information such as the driving behaviour or even an event. On the contrary, some legal bases might oblige employers to install tracking technology in vehicles to ensure the safety of employees for instance, or even to have a legitimate interest in being able to locate the vehicles at any time. Even in this case, Opinion 249/2017 outlined the possibility to find a balance between the two different needs, such as the one-off keeping in a "break-the-glass" way all that data necessary in case of accident or activating those tracking tools only during working times.

In Opinion 2/2017, the continuous monitoring of employees with those tools creates a serious issue for their privacy, that it has developed a fair balance based on the use of other methods, "such as the installation of equipment that prevents the use of mobile phones, as well as other safety systems like an advanced emergency braking system or a lane departure warning system", able to prevent inappropriate situations.

To conclude, any form of continuous employees monitoring, and surveillance must present a clear nature and be given to the employee in advance; should be limited in time and in terms of the number of people having access to it; must have a valid justification; and must not be based on directly accessing systems but, instead, must be based on less intrusive methods and measures.

The last two scenarios that Opinion 2/2017 mentioned are related to the employee's data disclosure to third parties, which is considered legal only if in the employer's legitimate interest[111] since employees do not have the power to give free consent, and to internal transfer

[111] As it is mentioned in Article 7 (f) Regulation 2016/679/EU.

to HR data, which could take place only if an “adequate level of protection” and intended purposes are ensured, as outlined on the Opinion 8/2001.

## 2.5. The “Transparency” Law Decree

On 13 August 2022 Legislative Decree No. 104 of 27 June 2022 implementing Directive (EU) 2019/1152 of the European Parliament and of the Council of 20 June 2019 on transparent and predictable working conditions in the European Union entered into force, which introduced additional information requirements if the employer uses "automated decision-making or monitoring systems to provide guidance relevant to the recruitment or assignment, management or termination of employment, the assignment of tasks or tasks as well as incident indications on the monitoring, evaluation, performance and fulfilment of the contractual obligations of workers"[112].

As for the use of decision-making systems, the rule does not introduce any novelty being such compliance already required (albeit with a lower degree of specificity) by art. 13 of European Regulation 679/2016 (GDPR), paragraph 2 lett. f) obliges the Data Controller to provide the data subject with information about "the existence of an automated decision-making process, including the profiling referred to in paragraphs 1 and 4 of Article 22, and, at least in such cases, significant information on the logic used, as well as the importance and expected consequences of such processing for the data subject". This information should therefore already be present in all the information on the processing of data prepared under art. 13 gdpr, even in those intended for employees. What is not insignificant, however, is the obligation of the employer to inform the employee throughout the report on the adoption of automated monitoring systems.

The use of such particularly invasive monitoring systems that we have mentioned in this chapter raises a question of the lawfulness of the processing of personal data carried out through

[112] Questions of interpretation and application regarding data protection related to the entry into force of d. lgs. 27 June 2022, n. 104 on transparent and predictable working conditions (c.d. Transparency Decree).

them, considering the sector discipline regarding the use of technological tools in the workplace[113].

The specificities of the technologies of these systems, as well as the nature of the data processed and the functionalities that are often associated with them, raise doubts as to the proportionality of their use and their compatibility with the general principles of data protection and with the framework of guarantees of freedom and dignity of workers, since, however, it is contrary to the national provisions prohibiting the employer from processing information relating to the worker's private sphere[114].

As regards the relevant data protection profiles, the new information requirements are foreseen if the employer uses automated decision-making or monitoring systems to provide guidance relevant to the recruitment or assignment, management or termination of employment, the assignment of tasks or tasks as well as incident indications on the monitoring, evaluation, performance and fulfilment of the contractual obligations of workers. Think of the adoption of an electronic attendance system (which eventually interfaces with a management system that can also be accessed by the human resources office) even if it provides for the start of work activities remotely or at a location other than the company; video surveillance of the places where the worker works; detection of the position of the worker through the completion of a certain action (loading or unloading packages; separate collection) through a handheld, electronic bracelet or other wearable devices; activity monitoring in smart working; email or video conferencing management (if company systems are used).

The decree substantially amended Legislative Decree 152 1997, which already provided for the obligation for the employer to give the employee all the information concerning his employment relationship but also allowed a generic reference to the contractual documentation. The fulfilment becomes more detailed, and, above all, it is addressed to all types of subordinate and para-subordinate relationships, therefore it also concerns coordinated and continuous self-employment relationships, occasional employment relationships referred to in article 54-bis of Dl 50/2017, and a sector that is usually excluded like domestic work.

Among the additional information that the employer, as data controller, must provide to the data subject are: the aspects of the employment relationship that are affected by the use of automated decision-making or monitoring systems; the functioning of the systems; the main parameters used to plan or train automated decision-making or monitoring systems, including

[113] See. Art. 114 of the Code, which refers to Art. 4 of L. 300/1970.
[114] See. Art. 113 of the Code, which refers to Art. 8 of L. 300/1970.

performance assessment mechanisms; the control measures taken for automated decisions, the correction processes, if any, and the quality management system manager; the level of accuracy, robustness and cybersecurity of the automated decision-making or monitoring systems and the metrics used to measure those parameters, and the potentially discriminatory impacts of the metrics themselves.

Given that the use of such systems may involve the processing of information directly or indirectly associated with employees, it is in any case necessary for the controller to verify the existence of a suitable condition of lawfulness (cf. Art. 5, par. 1, lett. a) and 6 of the Regulation) before processing the personal data of workers through such systems.

The employer, the data controller, must therefore respect the conditions for the lawful use of technological tools in the workplace as it has been established in the second paragraph of article 88 of the Regulation.

In particular, therefore, the existence of the conditions of lawfulness established by art. 4 of l. 20 May 1970, n. 300, referred to by art. 114 of the Code (the same paragraph 1 of art. 1-bis of the Decree expressly provides that "it remains without prejudice to the provisions of article 4 of the Law of 20 May 1970, n. 300") and respect for the provisions prohibiting the employer from acquiring and otherwise processing information and facts which are not relevant for the assessment of the employee's professional aptitude or otherwise relating to his private sphere (art. 8 of l. 20 May 1970, n. 300 and art. 10 d.lgs. 10 September 2003, n. 276, referred to by art. 113 of the Code). Articles 113 and 114 of the Code are considered, in the Italian legal system, more specific provisions and a greater guarantee of art. 88 of the Regulation, compliance with which is a condition of the lawfulness of the processing and the violation of which leads to the application of administrative fines pursuant to art. 83, par. 5, lett. d) of the Rules of Procedure.

The data controller is also required to respect the general principles of processing (art. 5 of the Regulation) and to implement all the obligations provided for by the legal provisions on the protection of personal data (also recalled by paragraph 4 of Art. 1-bis introduced by the Decree).

Paragraph 4 of art. 1-bis of Legislative Decree no. 152 of 26 May 1997, introduced by the Decree on Transparency, states that "In order to verify that the tools used for the performance of the service comply with the provisions laid down in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the employer or principal shall carry out a risk analysis and an impact assessment of the same treatments, by consulting the Data Protection Authority in advance if the conditions laid down in Article 36 of the Regulation

are met". The task of carrying out the risk analysis will be facilitated, if the attention of all the corporate figures who in various ways deal with privacy has already turned to the information to be provided to the worker, encouraging them to think carefully about the risks to which they are naturally exposed.

The rule in the comment introduces new stringent obligations for employers in their capacity as Data Controllers to the full benefit of the transparency of the employment relationship. Employees will thus be informed of the use of automated decision-making or monitoring systems to which they are subjected, and the Data Controller will have obtained a better awareness of the risks related to the treatments examined[115].

[115] L. Iadecola, *Adempimenti privacy e prime indicazioni operative dopo il decreto trasparenza*, Article: https://www.altalex.com/documents/news/2022/08/23/adempimenti-privacy-prime-indicazioni-operative-dopo-decreto-trasparenza, 2022.

# CHAPTER 3 – THE EVOLUTION OF REMOTE CONTROL IN THE WORKPLACE

## 3.1. The Power of Remote Control: Concept and Evolution

The technological and digital revolution that characterises today's information society is inevitably impacting the way companies do business and, consequently, on how employment contracts are executed[116], as we have mentioned in the first chapter. On the one hand, the organisation of work in an industrial enterprise increasingly involves the adoption of technological and computer tools necessary for the performance of work, on the other hand, new companies in the services and services sectors use information not only to make their production process more efficient but also as a commercial asset to generate value in the knowledge market.

Moreover, the process of technological modernization has developed together with a process of organisational flexibilization which has had as its main reflection a deconstruction of the relations of subordinate labour concerning the duration, the time and place of performance of the contract, as we have better analysed on the first part of this thesis. In the field of labour law, the answers to the requests for flexibilization and modernizer adaptation have been provided mainly through three "epochal" normative passages: the d.lgs. n. 276/2003 (reform "Biagi"), the n. 92/2012 (reform "Fornero"), the n. 183/2014 ("Jobs Act")[117]. They marked a departure from the traditional model of paid employment ( A rt. 2094 c.c.), often accentuating that asymmetry of power existing between employer and employee that the historical legislator had tried to balance with the approval of the Statute of workers (L. n. 300/1970). An asymmetry of power inherent in the prerogatives granted to the employer entrepreneur in the exercise of freedom of economic initiative (pursuant to art. 41 Cost.) and, therefore, the organisational autonomy guaranteed him from the ordering.

It is with regard to these legal powers that greater attention should be paid to defining the perimeter of protection of the workers included in the enterprise organisation so that the

[116] D. Garofalo, *Rivoluzione digitale e occupazione: politiche attive e passive*, in LG, 2019, n. 4, 329-349.
[117] A. Riccardi, *Flessibilizzazione dei rapporti di lavoro e destrutturazione dei sistemi,* in 2017 Annals of the Ionian Department in Legal and Economic Systems of the Mediterranean, University of Bari "Aldo Moro", DISGE, Taranto, 2017, vol. V, pp. 505-515.

balance between the fundamental principles of the legal system necessary to prevent that the entrepreneur's power of initiative does not run contrary to social usefulness or in a way that adversely affects security, to freedom and human dignity[118]. On the other hand, it has already been clearly stigmatised as "the violations of the rights of freedom consumed in companies do not have so much in the sign of contractual autonomy, but rather in the sign of organisational autonomy"[119].

Thus, the new information technologies in the working environment, now understood in a broad sense because of the increasingly blurred border, allow new types of data processing that have as the "side-effect" that greatly expands the possibilities of employers' control over work activities. These circumstances lead to "questioning the limits within which the employer can freely choose how to structure his company"[120].

Now daily, the news brings to light borderline cases in which the introduction of technological tools, albeit aimed at meeting legitimate business needs, appear detrimental to the dignity of the worker. Physical presence sensors, remote monitoring systems, "intelligent" video surveillance systems, wearable bracelets and software able to measure the timing of each work activity: these empirical examples are innumerable and illustrate the urgency of a change in mentality and approach to the problem.

The last interventions of the national and European legislators go in this direction, dictating a regulatory approach that, without any ambiguity, requires the operator of the law an integrated assessment of the work discipline and privacy. In the first place, with the EU regulation n. 679/2016, the European legislator intended to prescribe for all member states the standards of protection against threats to the fundamental rights and freedoms of citizens in the field of privacy, The European Parliament has a duty to ensure that the Member States are able to harmonise their internal rules. On the other hand, the rewriting of art. 4 of the L. n. 300/1970 (c.d. Workers' Statue), which took place about a year before the adoption of the EU regulation, made the exercise of the power of control conditional on compliance with the legislation on the processing of personal data, by an express reference to Legislative Decree no.lgs 196/2003 ("Codice Privacy")[121], making a definitive welding between the two regulatory complexes.

[118] C. cost. 9 March 1989, n. 103, in Rev. En. Dir. Lav, 1989, II.
[119] U. Romagnoli, *La prestazione di lavoro nel contratto di società*, Giuffré, Milan, 1967, 188 ss. L. Mengoni, *Lezioni sul contratto di lavoro*, Celuc, Milan, 1971.
[120] V. Nuzzo, *La protezione del lavoratore dai controlli impersonali,* Editoriale Scientifica, Naples, 2018.
[121] The decree entered into force on 1 January 2004, except for Articles 156, 176, paragraphs 3, 4,5 and 6, and 182, which entered into force on 30 July 2003, and was last amended by d. Igs. n. 101 of 10 August 2018, for the needs of harmonisation with Regulation (EU) 2016/679.

In the light of the new regulatory context, the organisational autonomy and the exercise of the employer's power of control require careful consideration with the legal safeguards placed to safeguard the values of the person.

In the course of the processing, we will try to give a brief account of the evolution of legislation on the control power of the employer, with particular attention to the regulation of the processing of personal data, in an attempt to offer interpretative solutions and new interpretative keys useful to determine the rules of conduct of the data controller employer appropriate to the specific case. The document considers the opinions and guidelines of the European data protection advisory bodies[122], as well as the decision-making practices of the Italian Data Protection Authority[123].

### 3.1.1. Powers of the Employer on Remote Controls

One of the fundamental bases of labour law is based on the necessity to rebalance the contractual weakness of the provider in the typical form of the employment relationship, which is mainly due to the fact that the law gives the employer powers of management, control and disciplinary against the other party. The object of this work is based on the power of control, under the law, to the employer in respect of its employees, to verify the exact performance with the prescribed diligence and observance of the precisions imparted.

What marks the difference between self-employment and subordinate employment lies in the worker's subjection to the executive, organisational and disciplinary power of the employer. Thus, the traditional configuration of the employment relationship gives the employer an active position of initiative and the employee a passive, subjection position.

The legislator of the Civil Code could not ignore the recognition that the implementation of such employment relationship is a potential source of danger also for the legal situation of the worker and has, therefore, indicated to the entrepreneurs the addition of necessary measures

[122] The advisory and guidance functions concerning the protection of personal data were carried out, in accordance with Directive 95/46/EC, by the Working Party pursuant to art. 29, also called Working Party art.29 (referred to by the acronym WP29), or an independent body, composed of a representative of the various national authorities in the field, in Europe.

[123] The role of the National Supervisor, already central under Directive 95/46/EC, is strengthened by Reg. EU No. 679/2016.

aimed at protecting the integrity of the worker, considering both the physical point of view but also the moral personality.

That is why in 1970 the Workers' Statue intervened, placing a barrier to the exercise of entrepreneurial powers, in particular, in Title 1, with the rules aimed at the protection of "Freedom and dignity of the worker" to give prominence to the legal involvement of the employee in the implementation of the relationship. The regulatory intervention responded many years in advance of the introduction of the "Privacy Code", to the specific needs of protection of the person who works and acts in a social area subject to the rules of power. In fact, the company is defined as a hierarchical organisation in which the worker has the duty to cooperate by virtue of the typical legal effect connected with the signing of the employment contract[124].

The fulfilment of the duties of work entails the necessary insertion of the obligor into a power structure (the enterprise organisation) in which the risk of compression of freedom and individual dignity is high, in view of the legal authority recognized by the "head of the enterprise"[125]. In particular, with regard to the main aspects relating to the protection of the confidentiality of the worker, which it is proposed to analyse below, there has never been any doubt that the employer had the power to monitor the worker remotely for the best "realisation of its technical-organisational interest"[126]. In fact, as stated by the most authoritative doctrine, the enterprise "can never be democratic", hence the need to introduce specific legal power of control of the employer, to prevent the worker from being subjected to continuous and pervasive controls, both inside and outside the workplace[127]. A risk made tangible by the massive use of technology in the workplace[128].

---

[124] M. Barbieri, *op. cit.*

[125] It is art. 2086 c.c. which defines the entrepreneur as the head of the enterprise and legitimises his hierarchical position (his collaborators depend on him hierarchically). Although the word head has been purged in an interpretative way of its original public incrustation, proper to the corporate ideology, as stated in an impeccable way by R. Voza, *La tutela del contraente forte nel diritto del lavoro,* in Rivista italiana di Diritto del Lavoro, fasc. 1, 2015, p. 15, the contractual relationship between the company and the work manifests an irrepressible peculiarity, that is to base and legitimise the supremacy of one contractor over another and, therefore, a position of private authority or, if you prefer, of private power.

[126] M.T. Carinci, *The remote control of the activity of the workers after the Jobs Act (art. 23 D. Lgs. 151/2015): ideas for a debate*, in Labour Law Issues, vol. 1, n.1, 2015, p. III.

[127] M. Napoli, *Quando un giurista racconta. A proposito de "Il lavoro in Italia" di Umberto Romagnoli,* Rivista Giuridica Del Lavoro E Della Previdenza Sociale, 1997, 529-534.

[128] Among the numerous cases reported in the past by the press, the control activity carried out by Fiat in the 1950s and 1960s through a specific supervisory body responsible for collecting information of all kinds on its employees, on aspirants, as well as on anyone who had political and commercial relations with Fiat. For further information on the case see B. Giudetti Serra, *Le schedature Fiat. Cronaca di un processo e altre cronache*, Rosenberg & Sellier, Turin, 1984.

The rationale of the 1970 statutory norm is found in the response to these needs of protection by limiting the exercise of the power of control. Although for the first time it formally acknowledges the existence of such a right in the hands of the employer, the Workers' Statute prescribes the cases in which it is prohibited and lays down a specific binding regime.

First of all, the statutory legislator has declared illegitimate the controls that go beyond the functional scope of the employment relationship, prohibiting without exception any employer ascertainment, both before and during the course of the relationship, "on the worker's fitness and disability due to illness or accident" (v. Art. 5, St. Lav.), "on the worker's political, religious or trade union views and on facts not relevant to the assessment of the worker's occupational aptitude" (v. art. 8, St. Lav.), even, going beyond the protection of what decades later will be called "sensitive data"[129].

Secondly, each employer is required to inform the workers concerned of the names and specific tasks of the staff responsible for supervising the work, thus prohibiting covert personal checks[130].

Finally, in the functional field, the statutory regulation ( Art. 4 St. Lav. ante novella), provided for the prohibition of the provision of installations for the purpose of "direct" remote control of workers, while subordinate forms of "indirect" control must be justified by the presence of worthy interests of the employer. The legislator would have "drawn a functional taxonomy of the devices usable by the employer", at the same time subjecting the installation to an authorization regime focused essentially on union control [131]. Art. 4 of Law No. 300/1970, therefore, condenses the judgement of disvalue compared to the remote controls carried out for the use of technological devices which, precisely because of their impersonality, are perceived as invasive and potentially damaging to human dignity[132].

The statutory provision, however, has shown with time its limits, whereas the guaranteed system established by it was de facto limited to prescribing the trade union agreement or the authorization of the Provincial Labour Directorate (now the Territorial

[129] The point observation is by M. Barbieri, *op. cit*., which highlights the farsightedness of the statutory legislator in guaranteeing workers the right to privacy.
[130] P. Tullini, *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro: uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali,* Volume 58 of Treaty on commercial law and public economic law, 2010.
[131] V. Nuzzo, op. cit., p. 34, defines the functionalization of the instruments (from which can derive as a side effect the control of the workers) to the satisfaction of qualified corporate interests.
[132] For a deepening on the original statutory discipline, ex plurimis cfr. B. Veneziani, *I controlli dell'imprenditore ed il contratto di lavoro*, Cacucci, Bari, 1975; G. Pera, C. Assanti, Commento allo Statuto dei diritti dei lavoratori, Cedam, Padua, 1972.

Directorate of the National Labour Inspectorate), as a condition of the legality of remote controls by employers, without specific measures to prevent private abuse[133].

The legal discipline, in fact, constituted at all the more the possibility that the agreement or the provision could foresee prescriptions regarding the use of the instruments and the systems (not finalised to the direct control of the workers but however suitable to realise it) but nothing on how the personal data collected are processed. In this respect, art. 4, St. Lav., had proved unsuitable for the worker's protection needs, since the neutralisation of any negative legal effect of the employer's (disciplinary) actions against the employee, as an outcome of the illegitimate remote control, has not offered sufficient guarantees to protect the confidentiality of the worker and has proved effective remedy only at the individual level of the employment relationship[134].

The evolution of the technological context during the decades following the introduction of the Workers' Statute has made unavoidable a rethinking of the regulatory discipline in the matter of controls both for the inability of the legal norm to "intercept" the new forms of control and for the need to harmonise the provisions of the privacy code. The inadequacy of the historical norm is evident if we only consider that, with regard to specific tasks, the new instruments are increasingly considered indispensable for the performance of work. In such cases, the inapplicability of the original art. 4, St. Lav, had argued that it appeared to make the use of equipment which was not part of the employment relationship subject to a binding regime only, and therefore not those which were indispensable for rendering the service. There is no doubt that IT tools and electronic communication services are now widespread in the most diverse working contexts and used for the proper performance of the work. They are tools that, in addition to fulfilling their function in view of the proper performance, also make possible the constant monitoring of work activities and the storage of large quantities of user data, greatly accentuating the risk of the worker being subjected to convert and "invasive" checks[135].

---

[133] A. Maresca, *Technological controls and worker protections in the new art. 4 St. lav.* , in P. Tullini (edited by), *Controlli a distanza e tutela dei dati personali del lavoratore,* Giappichelli, Turin, 2017, p. 3 ff. , speaks of malfunction of the original art. 4 St. lav. and the decline of the technique of protecting the confidentiality of the worker entrusted to the union agreement; for a former professional treatment of privacy profiles in the management of the employment relationship cf. M. P. Aimo, *Privacy, libertà di espressione e rapporto di lavoro,* Jovene, Naples, 2003; P. Chieco, *Privacy e lavoro*, Cacucci, Bari, 2000.

[134] A. Maresca, op. cit., p. 2.

[135] L. Tebano, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?,* In Rivista Italiana Di Diritto del Lavoro, 2016, 3, p. 345, work contexts, less intrusive, but more invasive, surveillance mechanisms are becoming more widespread.

These critical issues have not made it possible to postpone further a regulatory restyling, which came forty-five years after the introduction of the statutory rule on remote controls, with a complete reformulation of the legal text on the occasion of the extensive reform project, initiated by the delegated law n. 183/2014 and implemented by a plurality of successive legislative decrees (c.d. "Jobs Act")[136].

Specifically, the complete rewriting of art. 4 of Law No. 300 of 1970 was made by art. 23, co.1, of d. lgs. n. 151/2015, that it has released a new balance between the productive technical interest of the employer to control the punctual performance of the work performance and the interest to the dignity and the privacy of the worker sanctioned from our Constitutional Charter (art. 2 and art. 41, paragraph 2, Cost.), the European Convention for the Protection of Human Rights and Fundamental Freedoms (art. 8 ECHR) and, later, Regulation (EU) 2016/679 of the European Parliament and the Council, of 27 April 2016 (c.d. "GDPR")[137].

### 3.1.2. The "Old" Article 4. L. 300/1970

In 1970, a new important article has been introduced in our legal system by the Workers' Statute, aimed at safeguarding the personality rights of the worker[138]. The seventies, crossed by hard social battles and armed struggle, have left this statute, fundamental for those who work, the law of 20 May 1970 n.300, emblematically entitled "Rules on the protection of the freedom and dignity of workers, trade union freedom and trade union activity in the workplace and rules on placement", which provides that the powers of the employer are limited and subject, in turn, to control[139].

---

[136] For their complete examination cf. E. Balletti, D. Garofalo, *La riforma della cassa integrazione guadagni nel Jobs act*, Cacucci, Bari, 2016; E. Ghera, D. Garofalo, *Organizzazione e disciplina del mercato del lavoro nel Jobs act,* Cacucci, Bari, 2016.

[137] Indeed, the right to confidentiality is not expressed in the Italian Constitutional Charter and its classification as fundamental rights is derived from the systematic interpretation of the constitutional principles inherent in human rights. For further information v. L. Califano, *Tecnologie di controllo del lavoro, diritto alla riservatezza,* in P. Tullini (edited by), *Controlli a distanza e tutela dei dati personali dei lavoratori,* Giappichelli, Turin, 2017, p. 166 ff.

[138] A. Di. Stasi, *Diritto del lavoro e della previdenza sociale,* Giuffrè, Milan, 2011.

[139] A. Giuliani, S*orvegliare e punire,* edited by A. Di. Stasi, *Sul rapporto di lavoro*, AE, Ancona, 2016.

The innovations introduced were many: with art. 1 the freedom of opinion of the worker was established, which basically could no longer be discriminated against or dismissed for his political or religious views. Art. 2, however, provides us with another important rule at the time considered the heart of the law, that is the prohibition for the employer to use security guards to control the activity of employees. While art. 4 prohibits the use of audio-visual equipment; more specifically, the first paragraph states: "The use of audio-visual equipment and other equipment for the purpose of remote control of workers' activities is prohibited".

The first hypothesis, contemplated by the law, therefore, is that the exercise of control is carried out to distance the activity of the workers for the means of equipment and audio-visual systems. The absoluteness of the prohibition accompanying the legislative provision is part of that line of protection of the human values of the person of the provider who is involved in the contractual relationship and which the statute intends to protect. That is why this prohibition is aimed at eliminating a type of control over the work activity considered detrimental to the dignity and confidentiality of the employee, because of its continuity and its viability without the worker's knowledge. The ban does not remove any power of control over work, the eligibility of which is inherent in the scheme of the employment contract. The prohibition concerns the use of audio-visual equipment or any other equipment that allows the remote control of the work activity, namely a control characterised by its constancy or its feasibility at any time without the worker's knowledge. It is precisely by virtue of the first paragraph that the subjective right not to be controlled unlawfully requires that the control remains in its potential state and does not at all fall within the scope of the instrumental means of work organisation. This means that the employer will not be able to use the control tool for disciplinary purposes, which is intended for a purpose other than that of affliction.

Continuing, with the second paragraph we speak of the consent to install plants made necessary by organisational and productive needs or by work safety, even if they might prohibit the possibility of remote control in the first subparagraph. This consequence must, however, only be accidental or, as has been said, prejudiced, so that any findings relating to work are unusable. The existence of justifying requirements is not sufficient for the lawful installation of tools from which the possibility of remote monitoring of work performance may also derive, requiring an additional condition consisting of an agreement with the RSA or in the absence of these, with the internal commission.

This is a further guarantee that the sacrifice of the interest in confidentiality is allowed only where really necessary and, above all, is contained as much as possible by fixing how the equipment is to be used. The agreement with the internal commission is allowed only in the

absence of the RSA, and not in case of failure to agree with these. Where more than one RSA is established, agreement shall be reached with all. Individual employees have the possibility to challenge, even by emergency procedure, before the ordinary court the agreement reached with the employer, claiming that it is unlawful for the absence of the justifying requirements of the installation of the equipment. In the absence of an agreement, the employer may call on the Labour Inspectorate to ascertain the necessity of the installations in question for the subsistence of the requirements of the law, specifying where necessary the methods of use.

Recourse to the Inspectorate is inevitable in the absence of the RSA and the internal committee. Where they exist, the employer can only apply to the Inspectorate if he proves that he has already tried to reach an agreement with loyalty and good faith. The hierarchical appeal to the Minister of Labour is allowed only to the subjects indicated in the fourth paragraph (employer, RSA or, in the absence of these, internal commission or unions referred to in art. 19 St. lav.), and not to individual workers[140]. Violations of the rules in question constitute an offence pursuant to art. 38 St. lav. The active subjects of this contravention, not being an own crime, are not only the employers but also the operators of the prohibited installations.

From the civil point of view, it is certain the unusability of the investigations on the working activity deriving both from the use of the prohibited plants and from the use of the plants allowed to other finish[141].

This art. 4 was and still is located in Chapter I, Title I of the Workers' Statute, which therefore contains a set of provisions aimed at restricting the exercise of that power.

Over time, the use of new information technologies has led to an arrest in the growth of forms of control over the employee, feeding the existing imbalance of the contractual force of the employment relationship. The fundamental criterion of the processing of personal data, namely the defence of fundamental rights and freedoms and the dignity of the person concerned, was therefore inseparable from an overly open interpretation of the power of employer control. The search for the right balance between the claims of employers to exercise supervisory power and the protection of the confidentiality of the employer found a way in the principle of proportionality, by virtue of which the control activity is admissible only if it is used taking account of the opposing interests and placing as little burden on the rights of the individual first as such and then as a worker.

---

[140] Against the measures of the Labour Inspectorate, referred to in the second and third paragraphs above, the employer, the company union representatives or, in the absence of these, the works commission, or the workers' unions referred to in art. 19 may appeal to the Minister for Labour and Social Security within 30 days of notification of the measure.

[141] G. Giugni, *Lo statuto dei lavoratori commentario*, Giuffrè, Milan, 1979.

### 3.1.3. The “New” Article 4. L. 300/1970

With Law 183 of 2014 (c.d. Jobs Act.), the legislator wanted to reform, in essence, almost all the areas of labour law. With the term Jobs Act, in fact, there is an informal reform of labour law in Italy, (promoted and implemented by the Renzi government) aimed at making the labour market more flexible and adopted with the aim of reducing unemployment.

Article 23 of Legislative Decree No 151 of 14 September 2015, entitled "Simplifications in the field of work and equal opportunities", introduces new rules on audio-visual equipment and other means of remote control of workers, by amending Article 4 of Law 300 of 1970. This delegation concerns the reorganisation of the contractual forms and the inspection activity, aimed at strengthening the opportunities for entry into the world of work and rationalising existing employment contracts to make them more consistent with the current needs of the employment and production environment, as well as making inspection more effective; but above all it provides for the redefinition of the existing rules on remote control of workers.

The provision is finalised to give performance to the criterion of delegation of which to article 1, paragraph 7, letter f, of the delegated law 183 of 2014, which previews a "review of the rules on remote controls on plants and work tools, taking into account technological developments and balancing the production and organisational needs of the company with the protection of the dignity and confidentiality of the worker".

The need for a reform of the subject had in fact been underlined by much of the doctrine already during the eighties; in particular there was a need to adapt the regulations of company controls to new technologies[142]. By now, each technological tool is a means of performing one’s work and a means of control in the hands of the employer; moreover, the possibility of collecting data on its employees, even if they will not be used for disciplinary purposes, it allows to reconstruct a particularly precise profile of the worker, knowing his habits, opinions and orientations[143].

[142] F. Carinci, *Rivoluzione tecnologica e diritto del lavoro*, UTET, Turin, 1985.
[143] M.T. Salimbeni, *op. cit.,* notes that the old legislation was not able to accommodate in its field of operation, and therefore to counteract, the potential for invasive and massive control resulting from the technological revolution; the employer’s control had become more pervasive and potentially more insidious as intrinsic to work. The reform of Article 4 of the Workers' Statute: the ambiguous resolve of the legislator, riv. ita. lav., fasc.4, Milan, 2015, p. 589.

The reform has therefore introduced many interesting innovations, but not going to upset the structure of the old version. The questions raised by the jurisprudence's interpretation of the old rule will probably remain and will remain the concerns of those who see in every form of control over the conduct of work a dangerous source of instrumental initiatives of the employer. We cannot really speak of a real revolution because the key principles of the old discipline remain alive, especially the prohibition of direct control and the obligation of union agreement for the unintentional. It can be said, however, that the aim is to adapt legislation enacted almost fifty years ago to the technological innovations that now characterise every working relationship, always keeping at the centre of the opposing needs of the two parties.

The old art. 4 laid down a general prohibition on the remote control of workers; the same rule allowed only checks carried out by means of instruments used for organisational, production and safety purposes, allowed only after having entered into a prior agreement with the RSA or with the Internal Commission, or in the absence of agreement or RSA, the checks were allowed only with the permission of the Labour Inspectorate. Since it could happen that the workers could also be controlled with these instruments, the jurisprudence has coined for these controls, the term "pre-trial checks".

The jurisprudence has extended the possibility to carry out controls in spite of the general prohibition of art. 4, also in cases beyond the organisational, productive and safety purposes indicated above and even in the absence of the prior agreement with the RSA or the prior authorization of the labour inspectorate. In particular, the case-law has deemed the control by the employer legitimate in cases where the company's assets were in danger, identifying a particular category of control defined as "defensive".

This type of control was considered at first legitimate and allowed without limitation, with the Cass. Sez. Lav judgement. 15892/2007[144] The possibility of recourse to the defensive control defined above was limited only if the same did not concern the working activity of the employees and did not infringe the rights protected by art. 4 St. Lav. In this context application of the standard, which remained unchanged for 45 years from its first adoption, came into force the new art. 4 St. Lav. with the stated objective of updating the standard to the evolution of technology that today makes available to the employer numerous tools that are potentially suitable to capture, intentionally or accidentally, a large amount of personal data, currently widely protected by the Privacy Code (D. Lgs. n. 196/2003).

[144] The Court declared that the category of defensive controls had to fall within the discipline of the second paragraph of Article 4, therefore of those controls that need union authorization to be carried out, Law and practice of labour, Assago, 2007.

In the new first paragraph of art. 4 There is no longer the express prohibition of remote control of the activity of workers provided for in the previous art. 4, even if the prohibition still exists. In this new paragraph it is clearly stated that the installation of audio-visual equipment and other instruments is permitted, which also makes it possible for workers to be remotely controlled only for specific purposes (organisational and production needs, for the safety of the job and the protection of the company patrimony) and are specified the modalities to follow in order to be able to make it. According to the new paragraph 1, to guarantee the workers, it remains necessary to conclude a trade union agreement and in the absence of such agreement the prior authorization of the DTL (Directorate Territorial of Labour). In terms of agreements and authorizations, innovations have been introduced, namely that in the case of enterprises with production units located in different provinces of the same region or in different regions, the employer will be able to conclude the agreement with the trade union associations that are comparatively more representative at national level and, if there is no agreement, with the prior authorisation of the Ministry of Labour and Social Policy.

Another important novelty is that, in the second paragraph of art. 4 St. Lav., it has been clarified that the limitations and procedures described above do not apply with regard to the use of other tools that the employer assigns to his employees for the performance of the work (for example, computers, telephones, tablets as long as they are assigned to the individual worker or even to several workers but with personalised access for each, credit cards, telepass) as well as tools for the detection of access (e.g. in research, design and experimentation centres) and attendance (c.d. badge readers), even where they potentially give rise to the possibility of remote control of the employee. In this case, therefore, there is no obligation for the employer to reach a union agreement or to obtain administrative authorization: the control is free and can be carried out even without an organisational or productive need. Therefore, it will be up to the individual worker to check whether the control is exercised by the entrepreneur in a legitimate way and possibly go to a union or a lawyer to protect their rights.

Also for these reasons, in the last paragraph of art. 4 it has been clarified that the employer may use the information collected through the exercise of the power of remote control as well as the tools used by the employee to render the benefit, for all purposes related to the employment relationship, provided that workers are adequately informed of the manner in which the equipment granted is to be used (e.g. if intended for private or business use or mixed use, if their use is tolerated or prohibited within the undertaking). The methods by which the control will be exercised and always in compliance with Legislative Decree No. 196/2003, c.d. privacy code (e.g., specifying the information that is subject to temporary storage, the duration

of data retention etc.). In these cases, therefore, once the employer has provided its employees with adequate information about the company disciplines and rules regarding the use of emails, mobile phones, of PCs etc., on how to carry out checks by the company, and has complied with the privacy regulations, the items collected through such equipment may also be used in order to verify the diligence of the employee in fulfilling his obligations, with obvious disciplinary implications. If, however, the worker is not adequately informed of the existence and use of the control equipment and the methods of carrying out the checks, the data collected will not be used for any purpose, even for disciplinary purposes.

### 3.1.3.1. Instruments Involved in the Reform Process: Distinction between the Standard «Working Tool» and «Control Tool»

Important issue to be addressed in the light of the new legislative text of art. 4 St. lav. is the distinction of the field of application of paragraphs 1 and 2 that entails a difference of discipline applicable to «remote control instruments», paragraph 1, or to the instruments from which a remote control of the worker derives, but which are at the same time «work tools» or «detection of access and attendance», paragraph 2. Only in the first case, the installation or delivery must be preceded by the completion of the codetermination procedure in the union or administrative headquarters that ascertains the real existence of organisational needs, safety at work and/or the protection of company assets. In both cases, these are tools potentially capable of remotely monitoring the activity of workers but what makes the working tools such is that they are tools «used by the worker to render the work»[145].

It is evident that there is no attempt to catalogue the tools attributable to a certain type of work, since there is no a priori qualification of an instrument as a control equipment rather than a tool to render the work performance, but on the contrary, the recognition must take place according to the type of product and the characteristics of the work carried out. In general, the main purpose of using the equipment appears to be that, if directly instrumental to the performance of the service, it falls within the provisions of the second paragraph and therefore

[145] M. Marazza*, op. cit.*

benefits from exemption from the procedure in question. A current doctrinal[146] sees how the use of the tool by the worker must be effective, that is, it must be a tool concretely used by the employee and not merely granted or entrusted to him. Some doubts could arise in reference to "promiscuous" instruments, which in addition to satisfying organisational, safety and heritage protection needs, could also have a job at work.

Among the tools made available by the employer for organisational purposes, but that are not strictly necessary to make the performance include, according to commentators , we find the additional management computer programs inserted in computers, satellite tracking system for the protection of the company vehicles that are equipped with cars or corporate vehicles. These, while being supplied with the equipment of the employees, are not considered as tools used to render the work. They would therefore be part of those organisational measures or measures for the protection of safety and property which may give rise to control of workers who are subject to the constraints of the first paragraph, therefore are subject to prior agreement or authorization exactly as for the installation of cameras. Going on concrete examples, if the employer will deliver a PC the same will fall under the circumstances referred to in art. 4, paragraph 2 without the need for agreement; if, however, a management program capable of controlling the activity of the employee is installed in the PC, it will be necessary to proceed with the prior signing of an agreement with the RSA/RSU[147].

In other words, the tool itself used by the worker does not require authorization because it does not allow any control; when a system of possible control is added to it, it would be subject to the obligation of the union agreement or authorisation administrative. The delivery of a telepass or a fuel card in addition to the company car may also require the prior agreement, as a telepass and fuel card are necessary to the employer to simplify its management of travel and expenses refunds and from the examination of the invoice, cross-checked with the data of the employee's activity, the employer could remotely verify the correct fulfilment. However, if the instrument itself, with its intrinsic characteristics, is necessary to carry out the service, even if it is useful to the employer for organisational, safety and asset control purposes and enables the worker to be supervised, no agreement or authorisation will be required, but only compliance with the provisions of the third subparagraph. One could argue that GPS can be

[146] A. Rondo, *Checks on the employee's e-mail and art. 4 St. lav. Before and after the Jobs Act,* in Massimario di giurisprudenza del lavoro, 2016, p. 41.

[147] The restrictive thesis is from the Ministry of Labour and Social Policy: with a note dated 18 June 2015, it provided a very restrictive interpretation of paragraph 2 under consideration, affirming that the agreement or the authorization are not necessary if the instrument serves only the worker in order to carry out the performance, but instead become necessary when the instrument at the disposal of the latter is modified (ex: with a localizer software) so as to enable the employer to monitor the worker.

considered a tool used by the worker to make the work in the road haulage sector, with the consequence that the company could sanction the driver's illegal behaviour, according to the mapping that emerges from the GPS signal. But think, instead, for example, of those small companies that hire workers to distribute advertising in the mailboxes of private homes. In this case, it is obvious that the installation of a GPS device on the means of the worker engaged in sorting advertising sheets, would not be a working tool, but rather a control tool aimed at verifying whether the employee makes the advertisements regularly. In this case, the use of GPS would be unlawful, and the employer would commit a crime, as well as not being able to use the data obtained in disciplinary and compensatory action against the worker.

Since there are limited situations if doubts arise in the first application of the rule, we can only assume a path of reasonable prudence waiting to receive the first indications from the courts. The employer must, therefore, give to the worker adequate information about the methods of use of the instruments, the possibilities of control that can be carried out through those instruments, the methods by which the checks may be carried out and the purposes of the same specifying therefore also the disciplinary purposes and in compliance with the provisions of Legislative Decree no. 196/17 of 30 June 2003.

## 3.2. Protection of Workers' privacy: the Workers' Statute and the Privacy Code

The amendment made to Article 4 of the Workers' Statute by Legislative Decree 151 of 2015, as mentioned above, has created a very close link between labour law safeguards and safeguards that instead fall within the scope of the legislation on the protection of personal data. In particular, with paragraphs two and three, a very significant innovation has been achieved, both because a derogation from the obligation to agree referred to in paragraph 1 has been introduced with regard to "tools used by the worker to render the work" (cf. art. 4, paragraph 2, Stat. Lab.), and because from the date of entry into force of the reform (23 September 2015) the employer has the opportunity to use the information he has collected "for all purposes related to the employment relationship" (cf. art. 4, paragraph 3, Stat. Lab.), provided that the collection and use of such information have taken place in full compliance

with the provisions of Legislative Decree 30 June 2003, n. 196 containing the c.d. Privacy Code.

In particular, this latest development has given rise to a great deal of concern, particularly with regard to the protection of the employee's privacy and the risk of its being infringed by the employer. The scenario that we are analysing is always the one that derives from the need to balance two opposing needs, consisting, on the one hand, in the legitimate exercise by the employer of his power of control, and, on the other, in the necessity, for the worker, to see guaranteed and protected his rights of freedom and confidentiality.

It is therefore clear that it is appropriate to compare and, above all, to coordinate two different legislative models, such as the Workers' Statute, a specific expression of the desire to protect the worker as a weak part of the employment relationship, and the Privacy Code intended to be accompanied by the EU Regulation 2016/679.

From the necessary connection between the two disciplines emerges a first application problem, that is, whether the reference to the regulation of privacy contained in Article 4 should be considered limited to the regulatory framework of the Code or, conversely, extended to external sources. The reference is to the Guidelines issued by the Guarantor Authority pursuant to art. 154, paragraph 1, letter c of Legislative Decree 196/2003 on the processing of personal data of workers, recovered through the use of specific tools. Article according to which the Guarantor orders data controllers or processors to adopt such measures as are necessity or appropriate for the processing to comply with the provisions in force.

The task of Article 4 has always been to put a brake on the employer's supervision and at the same time to provide protection for the worker[148], a task that has not failed even after the amendment made by the legislative intervention in question. Moreover, we could even state that through the reference to the Privacy Code formulated by paragraph 3 of Article 4, these safeguards have probably been increased by finding their own regulation now in a text dealing specifically with this aspect of the employment relationship.

[148] C. Faleri, *Poteri di controllo del datore ed accertamenti sanitari sul prestatore di lavoro,* edited by C. Zolli, *La tutela della privacy del lavoratore,* Padua, 2000.

### 3.2.1. The Effect of the new General Data Protection Regulation on the power of Remote Control

In the past, worker consent based on the legality of processing has sparked widespread debate in the field of remote worker control. The contractor's consent cannot constitute a legal basis for remote control. This question must now be revisited in the light of new Art. 4 Workers' Statue, which imply supplementary standards and reference to the new regulations.

The legality of remote control over work must be based on the employer's need to pursue a "legitimate interest", provided, however, that the "interests or fundamental rights and freedoms" of the employee who need it do not override the protection of personal data, according to Article 6 (page 1, lett. f, registration number). Paragraph 1 of Art. 4 of Workers' Statue identifies tools deemed "legitimate" in the interest of the employer when it comes to essential business needs, qualifying in the organisation, production, safety at work and protection of company assets. This assessment must be shared with trade union or administrative organisations legalised by the same legal provisions. The instruments to provide or record access and frequency are fixed in paragraph 2 article 4 of Workers' Statue, not bound by the program. However, this does not mean that the control deriving from such instruments can be released from the satisfaction of the legitimate interests foreseen by art. 6. Letter. f, registration. It is therefore essential that the «legitimate interest», the controller is liable to prosecution only in the dimore of indirect controls and the balance between the legitimate interest of the employer and the rights of the providers, should be guided by applying the principles of «purpose limitation»[149] of «minimization»[150] and «transparency»[151].

It is therefore stated that the employer's interest is «legitimate» if the pursuit of the purpose invoked could not have been achieved with a less invasive type of control and, therefore, the employer has respected the principle of proportionality.

[149] Art. 5, GDPR, principle of «purpose limitation»: the employer is required to determine a lawful purpose of processing before its commencement and to respect it for the duration of processing. The Regulation provides for the use of the data collected also for «purposes different» from the original ones, provided that they are «compatible» with the latter.

[150] Art. 5, GDPR, the principle of «minimization» of data: considers unlawful that processing whose purpose can be achieved through other methods of processing that prevent identification and make it possible only in case of need.

[151] Art. 5, GDPR, principle of «legitimacy, correctness and transparency»: it renders tractable and usable only those data whose formation conforms to the law. Therefore, it excludes the lawfulness of the collection and use of information already subject to prohibitions of processing, such as those provided for in art. 4 and 8 St. lav.

The principle of «transparency», which is a cornerstone of the new legislation on remote control, is explicitly announced both by art 5 of the GDPR., but also in the new text of art. 4 St. Lav. in paragraph 3, which provides that «the worker is given adequate information on the methods of use of the tools and the carrying out of controls»[152]. It is quite clear that the provision does not offer unambiguous rules on the limits of employer's consent to question the monitoring tool in order to acquire data which may also concern the work performance and its data sensitivity. In any event, the information is required by the new provision without prejudice to the unusability of the data recorded by the instrument and it must be considered that it must be provided to the worker for any instrument used and not, as might be inferred, only for those tools used by the worker to render the work performance.

It is also essential to understand when the information provided to the worker can be considered «adequate». It follows that the adequacy of the information given to the worker must be assessed only in each dimore, provided that it covers at least: a) what are the instruments present in the company or used directly or indirectly by the worker, which may give rise to a possibility of remote control of work; b) how the instruments provided by the employer can be used, especially with regard to the possible possibility of using those same tools for personal purposes; c) the methods in which checks can be carried out on the data recorded by the tool installed in the company and/or made available to the worker. The European legislator is no longer satisfied with the completeness of the information but demands that the processing of personal data and the purposes that make it necessary are comprehensible and predictable for the data subject in all their aspects.

Moreover, the provision requires that the information «be given to the employee», therefore the employer must provide proof of direct knowledge by the employee, by means which enable each worker to ascertain that he has been received individually.

[152] A. Ingrao, *Pandemia, Protezione dei dati personali, accertamenti sanitari, vaccini, green pass e dintorni,* Lavoro Diritti Europa n. 3/2021, p. 110.

### 3.2.2. Conditions to Make Remote Controls Compliant with the GDPR

The new statutory rule also makes the employer subject to the obligation to provide the employee with adequate information regarding "how to use the tools and carry out checks", as we have previously anticipated, and, in any case, compliance with the provisions of the Privacy Code is required. This other burden legitimates or not the controls and the consequent usability of the data collected through them: the information is required by the new provision on pain of the unusability of the data recorded by the instrument and it must be considered that it must be provided to the worker also about the tools that the employer has installed before the reform of art. 4[153].

In fact, the Authority for the Protection of Personal Data (beginning with the guidelines of 1 March 2007 on the use of e-mail and the internet in the workplace and passing through the vademecum published in May 2015) has repeatedly dealt with the processing of data related to the control of employees, such as video surveillance systems, control systems of company computers and geo-locators GPS[154].

In the context of these interventions, it was reiterated that the treatment must nevertheless respect some fundamental principles; first of all, the principle of fairness, according to which the processing of personal data must take place in compliance with the fundamental parameters of loyalty and good faith. This requirement emerges even more clearly in the context of the employment relationship, characterised by a physiological imbalance of the contractual parties that requires the qualified protection of the weak person (the worker) who must be informed in advance and a clear manner of the characteristics of the processing of data collected through the use of tools allocated to him for the performance of his work.

The principle of correctness comes, therefore, to intersect and be confused with the principle of transparency, which last pervades all the regulatory apparatus regulating privacy. It was stressed that this concept of transparency in the workplace should not be understood as knowledge of the individual control act, but as awareness, acquired through information, to be

[153] I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in Labour Law Issues, vol. 2, No.1, 2016.
[154] S. Giubboni, G. Bronzini, *La tutela della privacy dei lavoratori e la Corte di Strasbourg, oltre il Jobs Act,* Rivista critica del diritto privato, Jovene, Naples, 2018, p. 143.

controlled and how the control can be operated[155]. Compliance with the principle of transparency implies, in addition, that the employer must indicate clearly and in detail, how the instruments entrusted to the worker are to be used and to what extent or in what way the checks will be carried out.

In the principle of necessity, however, the Legislator requires that the data subject to processing be collected and recorded only for purposes determined, explicit and legitimate and used in other processing operations in terms compatible with those purposes, in the sense that it is necessary to verify the usability of other less intrusive forms of control and preventive forms of control.

The personal data collected, and the methods of their processing must then be relevant and not exceed the purposes pursued. In this way, the principles of relevance and not excess are summed up in the principle of proportionality, which requires that the information collected must be effectively functional to the purpose to be pursued and processed to the extent that the sphere of the single[156] is as minimally invasive as possible.

These are therefore very penetrating substantial limits, if understood and applied rigorously, that allow us to recover, at least in part, as the new text of art. 4 takes away from the worker in terms of the specific and differentiated protection of the weak policy[157].

## 3.3. Collection of Personal Data for Disciplinary Purposes: Case Study

In the light of the new art. 4 St. lav. It is necessary to ask whether the legal system today legitimises the collection of personal data if it is aimed at satisfying a disciplinary purpose. It should be remembered, first of all, that the rules concerning the «processing of personal data» of the worker are applied without any distinction of type and function for which the tool is used since it is sufficient that the instrument can collect that information[158]. To answer the question,

[155] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, in Rivista italiana di Diritto del Lavoro, n. 1, Giuffrè, Milan, 2016, p. 83.
[156] A. Del Ninno, *In force the reform of art. 4 of the Workers' Statute on Remote Controls: Legislative Decree No. 151 of 14 September 2015*, Workers' Privacy and New Rules, Law and Justice, 2015, p. 11.
[157] V. L. Calafa', *The limits arising from the regulation of the protection of privacy*, in A. Levi (edited by), the new art. 4 on remote controls, Giuffrè, Milan, 2016, p. 145.
[158] A. Ingrao, *op.cit*. p. 172.

we analyse two cases already mentioned above, but this time focusing on which are the lawful conditions to collect personal data. The first case will refer to a direct control on the work performance, made through a working tool (paragraph 2. Art. 4 St. lav.) without union mediation, while the second case will concern the same type of control exercised, however, through a control tool (comma1, art. 4 St. lav.), intended to meet organisational and productive needs.

The first case study of the doctrine reports the control model implemented by the distribution centre of Amazon, one of the largest e-commerce in the world. For an organisational choice, in the warehouse of Amazon, the goods are not stored in an orderly way, but there is a computer system that allows processing data thanks to which each worker can know the place of storage, the availability and characteristics of the products. Both in the case of the workers who arrange the goods that arrived on the shelves and for those who dedicate themselves to packaging, the performance of the work cannot disregard an essential tool for the fulfilment of the activity: a barcode reader with integrated GPS[159]. In this way, each area manager can monitor in real-time the data collected by the badge reader that concerns all the details of the work performance of each employee. Each worker therefore knows his or her level of productivity and, if the benefits are not in line with the standards required to achieve the objectives set, the area manager is authorised by Amazon to complete first informal and then formal recalls. The same data can be used, then, also in a positive way to indicate the worker's «best of the month». What we have seen is, therefore, a case of direct control over work performance, by an indispensable tool to carry out performance for organisational purposes, even for disciplinary purposes[160]. Whenever Amazon intends to behave similarly in Italy as well, it must face the regulations we have previously mentioned. Such behaviours of control would allow an invasive presence in the daily life of the worker, that certainly could undergo a continuous and persistent monitoring of their work performance even regardless of the use as a support in the performance of their duties. It is, therefore, necessary to mention the third paragraph of Art. 4 Workers' Statute, which specifies that the information collected by the devices may be used provided that the worker is adequately informed of the methods of use of the means of carrying out checks, and in compliance with the provisions of the current privacy legislation. However, the limit of use of the data monitored by the company seems to

[159] The quickest way to collect the products for which he is responsible, or it is associated with a monitor that guides the worker on how to pack by showing him cardboard models to create the boxes.
[160] A. Ingrao, *op.cit*. p. 173.

be the information given to workers, with the natural consequence that the employer, including Amazon, could not use for any purpose, not even disciplinary, the data collected by the control tools unless the appropriate statement is provided.

The second example is a case judged by the Supreme Court on the basis of the previous text of art. 4 St. lav. on the legality of the installation of a computerised system for the automatic detection of counter operations, which consisted of transmission via computer on a local server, accessible only from the office (...), of all data relating to the various transactions with customers, intended to be transcribed/printed in the «back journal»; the transmission concerned data relating to the nature of the transaction, the customer, the operator of the counter and was aimed at managing the daily accounting, which in turn allowed, in the event of an error, to identify the operator who had carried it out; the office manager could, at any time and in real time display on his personal computer the operations that were performed at the counters and follow them on screen; in this way the hierarchical superior could control minute by minute the activity performed by each individual counter worker and his performance, the uncertainties in performing the operations and the execution times[161]. Such a treatment is unlawful according to the confirmative principles of the treatment referred to in Art. 5 Reg. and, in particular, about the principle of purpose limitation, data minimization and data protection by design and by default. It is a control realised in contrast to primis of art 2 Cost. which protects the «dignity» of the person in social formation, as well as art. 41, c.2, Cost. which requires that the «dignity» of the worker be preserved in the face of the exercise of the freedom of enterprise.

The balance between the employer's needs and the protection of the rights of the worker's person would be nullified if the regular reconstruction of the person's behaviour for disciplinary purposes were legitimised. Also, in the reformed Art. 4 St. lav. the contrast of Title I of the Workers' Statute between the technological control exercised «at a distance» and human control implemented «in presence» (Art. 3 St. lav.) remains firm, from which it is derived that simultaneous control must be carried out exclusively by persons. To confirm this orientation, in the international context, are placed the indications that we have seen on privacy in the workplace art. 88 Reg.: the specific rules for the protection of security for the protection of workers' rights and freedoms must include «appropriate and specific measures to safeguard human dignity, the legitimate interests and the fundamental rights of the persons concerned»[162].

[161] Cass. 9 February 2016, n. 2531 cited by A. Ingrao, op.cit., p. 176.
[162] Art. 88, Reg. 2016/679/UE.

It is necessary, in this context, to mention the interpretation of «private life» provided by art. 8 of the ECHR[163], which also includes the protection of «professional life»[164] and which sets out the fundamental points to prevent computer surveillance of workers from being exercised in violation of the human rights guaranteed by the Convention[165]. It is considered, therefore, that the employer, to have a complete and exhaustive picture of the worker's efficiency, should verify his behaviour over long periods, but continuous monitoring is contrary to the principle of minimization of data which, as we have said, it states that the power to collect other people's data is limited to the minimum both about the amount of data and for the period in which the data is collected.

It can, therefore, be concluded that the disciplinary purpose that presupposes this type of processing is illegal and, consequently, its prosecution involves the unusability of the data collected under the combined provision of Art. 10 decrees of adaptation and Art. 4, c. 3, St. lav[166].

### 3.3.1. The Bărbulescu C. Romania Case Study

As regards the relationship between remote worker monitoring and disciplinary dismissal, it seems useful to recall the judgement issued by the Fourth Chamber of the European Court of Human Rights on 12 January 2016 in the case Bărbulescu c. Romania[167] which established the important principle that it is not contrary to the right to private life (Art. 8

[163] The Council of Europe, on 4 November 1950, signed the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), considered the central text on the protection of fundamental human rights. Art. 8 ECHR is aimed at defending the fundamental right of the person «to respect for private and family life, his home and his correspondence». Later, other specific rules were elaborated to safeguard the condition of the workers more adapted to the technological evolution.
[164] The «right to private life» was interpreted extensively by the EDU Court, which not only recognised the protection of the intimate and family life of the individual but extended the protection to the relationships that the individual intended for professional reasons. The protection of the worker's working life also involves the protection of electronic communications sent from the workplace.
[165] A. Ingrao, *op.cit*., p. 176.
[166] Ibidem, p. 178.
[167] Case No. 61496/08 - Bărbulescu c. Romania; ECHR Judgment 013 (2016) of 12 January 2016.

CEDU[168]) the employer's access to his employee's electronic correspondence, transmitted through the company account for private purposes and in violation of his obligations.

Bărbulescu, a Romanian engineer in the sales department of a company, had opened an account on "Yahoo Messenger" to maintain relationships with customers. Subsequently, the company carried out a check on that account, monitoring the chat conversations of his employee, and fired him after having disputed that he had used the company's internet service for personal reasons. The applicant, therefore, appealed to the national courts alleging in particular that the right to the confidentiality of his correspondence had been infringed and that the employer's access to his correspondence had been unlawful. He then appealed to the Court in Strasbourg. By decision of 12 January 2016, the European Court initially denied, by a vote against, the existence of a violation of Art. 8 of the ECHR, considering the legitimate balance operated by the National Courts between the privacy of the employee and the interests of the employer and, therefore, reasonable monitoring of the communications of the employee in the context of the exercise of disciplinary power.

The decision, however, immediately aroused a lot of criticism, having been highlighted by several parties that any company policy must provide a series of safeguards in favour of the worker, complying with the long-standing standards of protection of internet communications set by different sources of international.

law, including within the Council of Europe[169]. The question, at the request of the applicant, was then referred to the Grand Chamber, which, by a judgement given on 5 September 2017, overturned[170] the first decision, considering that, in the present case, Art. 8 of the Convention had been infringed.

The Grand Chamber first accepted a very broad notion of "private life", noting that art. Article 8 of the Convention protects the right to personal development and in this context recognises the right to lead an adequate social life, that is, the possibility for the individual to develop his own social identity. On the other hand, the notion of private life extends to professional activities, so that restrictions on the private life of the individual fall within the scope of art. 8 where we have repercussions on how the person constitutes his own social identity, developing his relations with others. These statements undoubtedly reflect the rationale that in 1970 had led the statutory legislature to circumscribe the power of control over

[168] Recognises the fundamental right of every individual to the protection of personal data, according to which processing according to the principle of loyalty must be guaranteed, for specific purposes and on the basis of the consent of the data subject or another lawful basis provided for by law.
[169] A. Trojsi, *Il diritto del lavoratore alla protezione dei dati personali,* Giappichelli, Turin, 2012, p. 684.
[170] Even if by majority and with the dissenting opinion also of the Italian judge.

the employer both on the negative side of its shielding from prying eyes and however not impartial, but also on the positive side of the guarantee of an intangible sphere of freedom, a precondition for development, as the Court of Strasbourg says, of its own social identity.

For the 1970 Statute, the subject of controls intercepts the dual dimension of dignity and liberty[171]: the statements of the European Court update this approach[172], comparing it with the technological dynamics in place and with "work 4.0"[173]. The Bărbulescu, therefore, could have a certain role in directing the Italian Court of Legitimacy in rewriting salient aspects of the matter of limits to the employer power of computer control after the 2015 reform, also in the light of the complex new phenomenology that the very rapid technological transformation constantly demands the attention of jurists[174].

Moreover, the decision in the comment reiterated some of the principles already stated in our legal system, as well as Euro-Union sources, confirming that an adequate balance of interests between the respect for the private life of the worker and the good performance of the company cannot be separated from the necessary affirmation of certain limits to the employer's power of control. More specifically, it is not sufficient for the employee to know the prohibition of the use of company resources for personal purposes, since the employee must be informed in advance of the possibility of the employer accessing the contents of his correspondence and of the arrangements for such monitoring.

The monitoring of communications must be justified by the need for protection linked to actual detectable and measurable risk elements, to avoid any control hypothesis being traceable, even if there is no evidence to that effect, the risk of damage to computer systems or the combating of illegal activities. Monitoring must be gradual, in the sense that any alternative, less intrusive methods of worker privacy available to the company to pursue the same purposes must first be considered.

---

[171] S. Rodota', *op. cit.*

[172] C. Colapietro, *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro,* Franco Angeli, Milan, 2017, pp. 439-469.

[173] The precedent of 16 February 1993, Niemietz v. Germany, must be mentioned in this connection, according to which 'there do not seem to be any grounds in principle for believing that this concept of private life excludes professional or economic activity, since it is in fact during the course of working life that the majority of individuals have a significant opportunity, if not the most important, to develop relations with the outside world».

[174] On which the Guarantor of Privacy is indeed able to often express in advance guaranteed guidelines thanks to the observatory it has as stated in the testimony of A. Soro, *Liberi e Connessi*, Codice Edizioni, Turin, 2016.

## 3.4. The Concrete Application of Remote Controls

As has been observed in the course of this research, the complex relationship between remote monitoring of workers' activities and the protection of their dignity and confidentiality, within the broader framework of the legislation on the protection of personal data, is undoubtedly one of the most insidious fields of labour law.

The direction towards which the Legislator intended to move, renewing the formulation of Art. 4 of the Workers' Statute, is framed within the framework of a tendency to overcome ontological forms of prohibition of remote control, due to the massive change in the context, characterised by the increasingly incisive and widespread presence of technological tools. This type of instrument, by its very nature, requires regulatory flexibility and a degree of adaptation that is difficult to reconcile with forms of prohibition that are prejudicial and out of context.

The advent of technology and its growing diffusion over the years within the working world have made the differentiation between a control tool and a work tool increasingly blurred and difficult to grasp, debasing the preceptive scope of a prohibition dictated regardless. This phenomenon, as in the past, must naturally take into account the fundamental need to protect the dignity and privacy of workers, with a view to a fair balance of interests at stake.

However, the changed regulatory framework and context, seem to trace the path of a new perspective of protection on the one hand and overcoming the prohibition of remote control, at least as outlined by the Legislator of the '70 on the other. The current wording of the provision, as part of a framework of increasing integration with the regulatory system placed to protect personal data, allows shifting the focus of the protected legal asset precisely on the data and information acquired by the controls. If the working tools and the methods of production themselves, in the light of the increasing development and pervasiveness of new technologies, are increasingly characterised by the ability to track and collect workers' data and information, the legal good to be protected and the subject of the system of rules must necessarily consist of those two elements.

This possible first and partial outcome of reasoning is also corroborated by all the concerns and issues raised by the doctrine and also emerged in the application, both with reference in the main to the original version of art. 4, which is about the current one and the prospects that the same poses. As regards the statutory version of the rule, as has been observed, the doctrine had exposed a series of essentially unresolved interpretative knots and related to a

greater extent to the silence of the norm on the usability of the acquired quantum thanks to the controls and the poor attitude of the same to the adaptation to the changed, and in constant evolution, a reference context, characterised by the increasing diffusion of technologies in the workplace and between working tools. Such original incompleteness had, moreover, caused the genesis of the category of jurisprudential creation of the c.d. defensive controls, which had been dictated by the need to legitimise a control and to consistently use all the information acquired in all those cases of repression of the illegal conduct of workers not otherwise found.

The new legislative formulation made in 2015, while on the one hand, had the advantage of bringing greater clarity together with a greater degree of compliance with the changed reference context, has, however, left several spaces and points for reflection, especially if one observes and analyses the relationship of the discipline in question with the whole system of rules for the protection of personal data, characterised by an undoubted degree of comprehension and by the necessary and consequent requests for integration with the more strictly labour regulations.

The field of application and the main interpretations of the new legislative framework can therefore be traced through the examination of the different positions of the various actors involved and concerning the many issues to be clarified. In particular, therefore, to grasp the innovative scope of the rules under consideration, it is considered necessary to examine the positions of those who in practice implement them.

### 3.4.1. Remote Control and Technological Implications

The possible effects and application declinations of the reform of art. 4 Stat. Lav. and its renewed and, in some ways, strengthened integration with the standard for the protection of personal data, can be read, in the first place, through the analysis and examination of several Measures of the Guarantor for the protection of personal data dictated, in which the Authority offers important food for thought.

In 2017, with Provision no. 138/2017[175] issued upon the outcome of a preliminary verification (fulfilment no longer provided for as governed by the previous Privacy Code following the full operation of the GDPR and the consequent adjustments to the national law), the Guarantor expresses its opinion on the adoption by an employer of a system equipped with a satellite-based location of company vehicles via a GSM/GPRS[176] connection to the "Data Centre" of an external company processing and making data available. It should be noted that the employer had already signed collective agreements with the trade unions. In particular, the system is dedicated to the management of timely intervention in the event of failure, the safety of workers c.d. in solitude, the management of the employment relationship in terms of loading and unloading time, the protection of company assets, and it also allowed, through the reporting, to know the distance covered, the average speed of the vehicles useful also to the distribution of the works and the journey times. The same system was activated only following the ignition of the vehicle by the worker; access to the data, moreover, was allowed only to specific subjects in charge of the processing.

The Guarantor, concerning the synthesised characteristics of the system, points out firstly that although it is not configured for the direct identification of drivers, in line with the principle of data minimisation, this possibility can be achieved by consulting the documents relating to onboard authentication carried out at the beginning of the working shift. The Guarantor also notes the lawfulness of the aims pursued with the installation of the system that is substantiated in the pursuit of organisational and productive purposes, work safety and the protection of company assets, by the first paragraph of art. 4 Stat. Lav. In the present case, the installed instrumentation does not qualify as a working instrument, not being pre-ordered to the performance of the service, with consequent repercussions in the sphere of application of the first paragraph of the statutory provision. It is also interesting to note the reference made in the Provision to Circular No. 2/2016 of the National Labour Inspectorate. For the considerations of the legality of the system, the Guarantor observes that the company has concluded two trade union agreements for this purpose, in which the installation of the location system in question is regulated for reasons of safety at work (identification of the C.D. man on the ground) and insurance protection of vehicles in case of theft. These agreements will, in the Authority's opinion, require the necessary additions relating to the additional purposes and the

[175] Garante Privacy, Preliminary check. Processing of personal data of employees carried out through the localization of company vehicles - 16 March 2017 [6275314] in: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/6275314.

[176] The term GSM is an acronym for Global Systems for Mobile. The term GPRS is an acronym for General Packet Radio Service.

related processing methods. The legal basis of the qualified processing by the Guarantor is identified in the legitimate interest of the purposes posed.

It is also necessary to note the physiological sensitivity posed by reference to the application of data processing principles: in particular, operations must comply with the principles of necessity, relevance and not excess concerning the aims pursued and also about the time of storage. The system itself will have to be configured in such a way as to detect the geographical position at intervals proportionate to the purpose.

The same Authority comes to similar considerations, admitting, in the preliminary verification and after the adoption of the requirements indicated therein, the lawfulness of the processing of personal data deriving from the collection of satellite coordinates relating to the geolocation of mobile and vehicular radio-electronic equipment. In Measure, No. 247/2017[177] The Guarantor stresses that the adoption of the geolocation system in question is based on organisational and production needs, safety at work and the protection of the company's assets through mobile radio devices and vehicle terminals. This equipment, activated by employees for the duration of working hours, therefore allows the processing of geolocation data. Clarified that the same data cannot be defined as anonymous, due to the possibility of association with an identifiable data subject, in the Provision it is evidenced as is also realisable from part of the society an indirect control on the workers allowing therefore also the reconstruction of the activity. The Guarantor also observes that it is necessary to apply, in addition to that relating to personal data, the working discipline with particular reference to the tools from which also derives the possibility of remote control under art. 4, paragraph 1, Stat. Lav.

The aims represented by the company, therefore, appear to be attributable to organisational and production needs, occupational safety and the protection of the company's assets represented by the same law and in the presence of which remote control is allowed after agreement with the trade unions or, in the absence, as in this case, administrative authorization. The possibility of access to the quantum of data collected reserved by the company to the Technical and Personnel Management is limited, as indicated by the same company, to the occurrence of repeated anomalies in the management of the service and to resolve them.

About the integration profiles between the legislation on data protection and the labour legislation in the strict sense, the Guarantor identifies the key to the relationship between the two subjects in the information obligations referred to in art. 13 of D. Lgs. n. 196 (in its

[177] Garante Privacy, Preliminary check. Processing of personal data deriving from the collection of satellite coordinates relating to the geolocation of electronic equipment of mobile and vehicular radio type - 24 May 2017 [6495708]. Website: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/6495708.

previous version) and art, 4, paragraph 3, Stat. Lav. that the company must respect to make employees fully aware of the processing carried out and the tools used, together with the methods used. Such processing must of course also comply with the principle of necessity, as regards the identification of data subjects, and must be limited to the pursuit of specific, explicit and legitimate purposes or any other purposes provided compatible.

The integration profiles between the work discipline and that of privacy, which imply a relationship of intrinsic bond and mutual and necessary respect, are further underlined in other measures issued by the Italian Data Protection Authority about vehicle geolocation systems or video surveillance tools that, although indirectly, also allow remote control of workers.

In particular, Measure No. 432/2017 admits the possibility, subject to the prescribed compliance, of the processing of data collected by a technological system that allows the location of smartphones and tablets assigned to the employees of a company to ensure its customers greater accuracy in quality control the distribution of advertising material. The Guarantor, in qualifying as lawful the purposes pursued by the company because they respond to the satisfaction of organisational and production needs under the first paragraph of Art. 4 Stat. Lav., emphasizes the conformity of the system regarding the enforced labour norm and welcomes positively the intention of the society to activate the authorization procedure in front of the competent centre of the Labor Inspectorate. The Measure also clarifies how the principles of necessity and proportionality are respected through pseudonymization techniques and predetermined and non-stop intervals of data processing and the circumstance of the warning of activation of the system to operators.

The intrinsic nature of the connection between data protection and the need to respect art. 4 also in terms of the unlawfulness of pervasive and constant control over performance, is highlighted for instance by Measure No. 427/2018[178], with which the Guarantor, the outcome of some inspections, confirms the unlawfulness of the processing carried out by a company in the context of waste collection, water transport and expulsion and carried out using a system of geolocation of company vehicles and video surveillance. Specifically, the system allowed to display in real-time the position of the vehicles, the driving time and the route. The company also provided a daily report containing the name of the driver and the routes to be carried out; compared to the described system, installed also because of the high crime rate in the areas, the

[178] Garante Privacy, Order of 19 July 2018 [9039945]. Website: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9039945.

employees had been invited orally to give their consent and there had been (at least in a first phase) the conclusion of an agreement with the trade unions. In confirming its assessment of illegality, the Guarantor, highlighting the characteristics of the plant that allows the constant collection of data on vehicles with an extremely frequent periodicity, notes the non-compliance with the principle of proportionality, which also concerns the regulatory framework introduced by the GDPR, based on the useful reachability of the same result with more limited treatment, and the excessive length of storage times. Contrary to what is required by the Privacy Code (in the previous version) and the GDPR, the processing does not even comply with the principles of necessity, relevance and not excess as it is suitable to carry out continuous monitoring of the activity of employees.

Another interesting measure has been taken by the Decision of 2 March 2023, in which the Guarantor for the protection of personal data has sanctioned a well-known brand of clothing for having installed and used video surveillance systems at a multiplicity of stores in the absence of an agreement with trade union representatives or authorization issued by the Labour Inspectorate under art. 4 of Law No. 300 of 1970 ("Workers' Statute"). In particular, the Data Protection Authority reiterated that under Art. 4 of the Workers' Statute, the video surveillance equipment, if from them derives "also the possibility of remote control" of the activity of employees, "may only be used for organisational and production needs, for occupational safety and the protection of the company's assets" and the relevant installation must, in any case, be carried out after the conclusion of a collective agreement with the unitary union representation or with the company's trade union representatives or, where such agreement has not been reached or in the absence of representations, only as preceded by the issue of appropriate authorisation by the Labour Inspectorate. For the Guarantor of the protection of personal data, the activation of this guaranteed procedure does not supplement a mere formality, nor can it be qualified as a simple documentary fulfilment. On the contrary, this procedure is to be considered an "indefectible condition for the installation of video surveillance systems" as it "protects collective and superindividual interests". In the absence of the union agreement or of the authorization of the Inspectorate of the job, therefore, the collective interests of the garrison in which they are placed must be considered damaged, as moreover confirmed also from the jurisprudence of legitimacy. In this way, the legislation tends to reduce the disproportion between the position of employers and that of workers. It is only through this procedure that the employer can assess correctly, through the intervention of the trade union representatives or the Labour Inspectorate, the ability to damage the dignity of workers of technological tools from which remote control of workers (such as video surveillance equipment) may result, as

well as the effective compliance of such equipment with technical, productive or safety requirements.

The possible absence of a trade union agreement or the authorization of the Labor Inspectorate, if necessary, however, also integrates a violation of the principle of the lawfulness of the treatment referred to in Art. 5, par. 1, lett. a) of EU Regulation 679/2016 ("GDPR") about the provisions of art. 88 of the GDPR itself and art. 114 of D. Lgs. 196/2003, as last amended by D. Lgs. 101/2018 ("Privacy Code"). The above-mentioned rules expressly state that processing of personal data carried out in the context of the employment relationship, to be lawful, must comply with the specific rules which the national law considers necessary for the "safeguarding the human dignity, legitimate interests and fundamental rights of the persons concerned", with particular reference to the prohibition of monitoring or monitoring work. In this regard, the Guarantor has clarified that the provisions of the GDPR and the Privacy Code are added (and do not replace or fail) to the provisions of the Workers' Statute or the Labour Inspectorate.

The Guarantor has reiterated that the areas of operation of the two disciplines (labour law and privacy), although connected, are autonomous. On the one hand, art. 4 of the Workers' Statute "the competence of the Labour Inspectorate to issue the administrative authorization necessary for the installation of audio-visual equipment and other tools from which also derives the possibility of remote control of workers for organisational needs; and productive, for the safety of the job and the protection of the company patrimony, concerning the profiles purely job-law". On the other hand, art. 114 of the Privacy Code "confers the competence of the Guarantor about the verification of compliance with the rules on the protection of personal data" in the field of employment relations, also about the regulation on remote controls.

As we have seen in previous cases, the lawfulness of the processing of workers' data should be verified in light of the general rules and conditions dictated by the regulatory norm. According to Article 6 GDPR, each data controller must first ensure that the related transactions have a legal basis in one of the following cases: the consent of the worker, the need for processing to fulfil the contractual relationship to which the data subject is party, the fulfilment of a legal obligation to which the employer is subject, the need for processing to safeguard the worker’s vital interest, the performance of a task in the public interest, the pursuit of its legitimate interest, provided that the interests or fundamental rights and freedoms of the worker do not prevail. The respect for the fulfilment and of the prescription's privacy which indispensable conditions for the usability of the information collected in the places of the job through technological instruments, previewed from comma 3, Art.4, In the first place, it

requires the identification of the conditions of lawfulness of the processing of data involved in the exercise of the power of control.

## 3.5. Concluding Remarks

Downstream of this research and investigation that has developed around the complex and a renewed relationship between the possibility of remote controls and the need to protect the confidentiality of workers within a working context characterised by constant progress concerning a new legislative provision which has recently been rewritten and to the aims underlying it, it is considered appropriate to outline some brief concluding considerations.

In the wake of a phenomenon of flexibilization of the employment relationship, with specific regard to its greater internal fluidity, and to adapt the statutory provision to the changed framework of reference, the Legislator wanted to seek a new and different point of balance between the prerogatives of employers and the fundamental requirements of worker protection, also pursuing purposes of rationalisation and simplification. A situation so different from the past, starting from the current wording of art. 4 Workers' Statue, has recorded the decided entrance of the regulations mail to the protection of the personal data of the worker who, for evidence, represents the new fulcrum object of the combined legislative one on which must concentrate the attention of the interpreter.

The described abandonment of the concept of prohibition of remote control for the benefit of usability for all purposes related to the employment relationship, within a new delimiting order implied by the balancing of interests, allows supporting a reparametrize of the point of equilibrium between prerogatives employers and requirements of the protection of the workers. The object of the legislative attention and the focal point of the new balance, therefore, seems to have focused on the protection of personal data, within a renewed discipline of interaction between the statutory provision and the legislation dictated to the protection of personal data, whose fundamental principles constitute the pillars on which the protection of the acquired quantum and the same legitimate expectation of privacy of the worker.

It has become evident that remote monitoring of workers can pose significant risks to privacy and workers' rights. Monitoring technologies, such as activity tracking software or

remote monitoring devices, can collect vast amounts of personal data without informed consent, jeopardising the privacy and autonomy of workers.

Existing regulations, such as the General Data Protection Regulation (GDPR), provide an important legal framework for personal data protection, but a more specific and targeted approach is required to address remote monitoring of workers. It is essential to consider the purpose of data processing, ensure compliance with principles of necessity, proportionality, and data retention limitation, as well as uphold workers' rights to information and privacy. Awareness and education are crucial to ensure that workers are fully informed about the types of monitoring they are subjected to and their rights regarding personal data protection. Organisations should provide clear and transparent policies regarding remote monitoring and involve workers in the decision-making process.

Furthermore, the development of technological tools and methodologies that respect workers' privacy is necessary, such as adopting a privacy-by-design approach and implementing anonymization and pseudonymization mechanisms for data. Organisations should conduct Data Protection Impact Assessments (DPIAs) to evaluate and mitigate privacy risks associated with remote monitoring technologies.

Lastly, legislators and regulatory authorities must be proactive in adapting existing regulations to specifically address the remote monitoring of workers. Clear and updated rules should be developed that balance organisational needs with workers' rights to privacy and autonomy.

At the same time, in addition to allowing this new perspective to emerge within a framework of constant technological innovation, the matter must necessarily continue to consider also with the requirements of rationalisation and simplification made explicit by the delegated Legislator. The positions described by the main actors called to apply the new statutory provision, characterised by the described interaction profiles and integration with the provisions on the protection of personal data, have shown the permanence of some elements of uncertainty that, although less than in the past, continue to characterise the material and its full response to the evolution of the world of work and its great transformation. In particular, the work of subsumption of the concrete case to the normative prototype continues to record, as we have previously seen, a series of oscillations and divergent positions between which, while not being translated into the ambiguities of interpretation of the past, the operators of a whole series of increasingly widespread technological instruments are experiencing difficulties of qualification, at the expense of rationalisation and simplification.

In conclusion, the protection of personal data in the employment relationship requires a combination of actions from organisations, legislators, and regulatory authorities. Only through a holistic and collaborative approach can a balance be achieved between technological innovation and the safeguarding of workers' fundamental rights in the context of new work models.

If, therefore, it is the task of the law to regulate an area characterised by phenomena of constant change because of the pervasiveness and the speed with which innovations intervene, it can well be said that the challenges to be met remain multiple and full of elements of complexity.

# BIBLIOGRAPHY


Aimo M. P., *Privacy, libertà di espressione e rapporto di lavoro,* Jovene, Naples, 2003.

Alvino I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in Labour Law Issues, vol. 2, No.1, 2016.

Balletti E., Garofalo D., *La riforma della cassa integrazione guadagni nel Jobs act*, Cacucci, Bari, 2016.

Barbera A., *La Carta europea dei diritti e la costituzione italiana*, in Aa.Vv., *Le libertà e i diritti nella prospettiva europea: studi in memoria di Paolo Barile*, Padua, 2002.

Barbieri M., *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse*), Volume Controlli a distanza e tutela dei dati personali del lavoratore, edited by P. Tullini, *Turin, 2017, pp. 183-208.*

Bellavista A., *Il controllo sui lavoratori,* Turin, 1995.

Bevitt A., Stack C., *Preparing for the GDPR - advice for employers,* in Privacy and Data protection Journal (PDP), vol. 16, issue 6, 2016.

Brino V., *Geolocalizzazione*, in *Lavoro e Tecnologie. Dizionario del diritto del lavoro che cambia*, edited by Borelli, S., Brino, V., Faleri, C., Lazzeroni, L., Tebano, L., Zappalà, L., Giappichelli, Turin, 2022, pp. 116-119.

Brino V., *Smart Working*, in *Lavoro e Tecnologie. Dizionario del diritto del lavoro che cambia*, edited by

Borelli, S., Brino, V., Faleri, C., Lazzeroni, L., Tebano, L., Zappalà, L., Giappichelli, Turin, 2022.

Bughin J., Livingston J., Marwaha S., *Seizing the Potential of Big Data,* Article McKinsey Quarterly Business Technology Office, October 2011.

Calafa' V. L., *The limits arising from the regulation of the protection of privacy*, in Levi A.(edited by), the new art. 4 on remote controls, Giuffrè, Milan, 2016, p. 145.

Califano L., *Tecnologie di controllo del lavoro, diritto alla riservatezza,* in Tullini P. (edited by), *Controlli a distanza e tutela dei dati personali dei lavoratori,* Giappichelli, Turin, 2017, p. 166 ff.

Carinci F., *Rivoluzione tecnologica e diritto del lavoro*, UTET, Turin, 1985.

Carinci M. T., *The remote control of the activity of the workers after the Jobs Act (art. 23 D. Lgs. 151/2015): ideas for a debate*, in Labour Law Issues, vol. 1, n.1, 2015, p. III.

Chieco P., *Privacy e lavoro*, Cacucci, Bari, 2000.

Colapietro C., Giubilei A., *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della Cassazione,* Labour & Law Issues, 2021, 7(2), pp. 186-209.

Colapietro C., *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro,* Franco Angeli, Milan, 2017, pp. 439-469.

Culot G., Nassimbeni G., Orzes G., Sartor M., *Behind the definition of Industry 4.0: Analysis and open questions*, International Journal of Production Economics, Elsevier, Amsterdam, vol. 226(C), August 2020.

Del Ninno A., *In force the reform of art. 4 of the Workers' Statute on Remote Controls: Legislative Decree No. 151 of 14 September 2015*, Workers' Privacy and New Rules, Law and Justice, 2015, p. 11.

Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro*, in Rivista italiana di Diritto del Lavoro, n. 1, Giuffrè, Milan, 2016, p. 83.

Di. Stasi A., *Diritto del lavoro e della previdenza sociale,* Giuffrè, Milan, 2011.

Faleri C., *Poteri di controllo del datore ed accertamenti sanitari sul prestatore di lavoro,* edited by Zolli C., *La tutela della privacy del lavoratore,* Padua, 2000.

Fcault M., *Sorvegliare e Punire, nascita della* prigione, Einaudi, Turin, 1975, p. 164.

Finocchiaro G., *Limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro, Web e lavoro. Profili evolutivi e di tutela*, P. Tullini, (edited by), Giappichelli, Turin, 2017, p. 60.

Finocchiaro G., *Privacy e Protezione dei Dati Personali, Zanichelli*, Turin, 2014, 151-152.

Galgano F., *Trattato di diritto commerciale e diritto pubblico dell'economia*, Cedam, Padua, 2008.

Garofalo D., *Rivoluzione digitale e occupazione: politiche attive e passive*, in LG, 2019, n. 4, 329-349.

Ghera E., Garofalo D., *Organizzazione e disciplina del mercato del lavoro nel Jobs act,* Cacucci, Bari, 2016.

Giubboni S., Bronzini G., *La tutela della privacy dei lavoratori e la Corte di Strasbourg, oltre il Jobs Act,* Rivista critica del diritto privato, Jovene, Naples, 2018, p. 143.

Giudetti Serra B., *Le schedature Fiat. Cronaca di un processo e altre cronache*, Rosenberg & Sellier, Turin, 1984.

Giugni G., *Lo statuto dei lavoratori commentario*, Giuffrè, Milan, 1979.

Giuliani A., S*orvegliare e punire,* edited by Di. Stasi A., *Sul rapporto di lavoro*, AE, Ancona, 2016.

Goodman B., Flaxman S., *European Union regulation on algorithmic decision - making and a right to explanation,* AI Magazine, New York, Vol 38, No 3, 2017.

Grandi M., *Rapporto di lavoro*, in Enc. Dir., vol. XXXVIII, Giuffrè, Milan, 1987.

Harrison G., Lucassen M., *Stress and anxiety in the digital age: the dark side of technology*, the open Learn University, UK, 2019.

Iadecola L., *Adempimenti privacy e prime indicazioni operative dopo il decreto trasparenza*, Article: https://www.altalex.com/documents/news/2022/08/23/adempimenti-privacy-prime-indicazioni-operative-dopo-decreto-trasparenza, 2022.

Ingrao A., *Pandemia, Protezione dei dati personali, accertamenti sanitari, vaccini, green pass e dintorni,* Lavoro Diritti Europa n. 3/2021, p. 110.

Khanna A., Khanna P., *L'età ibrida, il potere della tecnologia nella competizione globale*, Codice Edizioni, Turin, 2013.

Magone A., Mazali T., *Industria 4.0. Uomini e Macchine nella fabbrica digitale*, Guerini, Milan, 2016.

Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, CSDLE It., n. 300/2016, p. 7.

Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori,* in Rivista Italiana di Diritto del Lavoro, 2016, pp. 513-546.

Mengoni L., *Lezioni sul contratto di lavoro*, Celuc, Milan, 1971.

Napoli M., *Quando un giurista racconta. A proposito de "Il lavoro in Italia" di Umberto Romagnoli,* Rivista Giuridica Del Lavoro E Della Previdenza Sociale, 1997, 529-534.

Nuzzo V., *La protezione del lavoratore dai controlli impersonali*, Editoriale Scientifica, Naples, 2018.

Oshri I., Kotlarsky K., Willcocks L., *The Handbook of Global Outsourcing and Offshoring*, 3rd edition, Palgrave Macmillan, London, 2015.

Paissan M., *La privacy è morta, viva la privacy*, Ponte alle Grazie, Florence, 2009.

Pera G., Art. 4, in C. Assanti, Pera G. (edited by), *Commento allo Statuto dei diritti dei lavoratori,* Padua, 1972.

Pera G., Assanti C., *Commento allo Statuto dei diritti dei lavoratori*, Cedam, Padua, 1972.

Riccardi A., *Flessibilizzazione dei rapporti di lavoro e destrutturazione dei sistemi,* in 2017 Annals of the Ionian Department in Legal and Economic Systems of the Mediterranean, University of Bari "Aldo Moro", DISGE, Taranto, 2017, vol. V, pp. 505-515.

Riso S., *Monitoring and surveillance of workers in the digital age*, European Foundation for the Improvement of Living and Working Conditions, 2021.

Romagnoli U., *La prestazione di lavoro nel contratto di società*, Giuffré, Milan, 1967, 188 ss.

Rondo A., *Checks on the employee's e-mail and art. 4 St. lav. Before and after the Jobs Act,* in Massimario di giurisprudenza del lavoro, 2016, p. 41.

Salimbeni M. T., *Nuove Tecnologie e rapporto di lavoro: quadro generale*, in R. De Luca Tamajo- R. Imperiali D'Afflitto, R. Romei, *Nuove tecnologie e riservatezza del lavoratore*, Franco Angeli, Milan, 1988.

Soro A., *Liberi e Connessi*, Codice Edizioni, Turin, 2016.

Soro A., *Persona, Diritti, Innovazione. Discorso del Presidente* - Report of the year 2016, Guarantor of the protection of personal data. Cfr. the entire report presented by the Garante on 6 June 2017 at the Sala della Regina in Palazzo Montecitorio.

Tebano L., *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?,* in Rivista Italiana Di Diritto del Lavoro, 2016, 3, p. 345.

Trojsi A., *Il diritto del lavoratore alla protezione dei dati personali,* Giappichelli, Turin, 2012, p. 684.

Tullini P., *Controlli a distanza e tutela dei dati personali del lavoratore,* Giappichelli, Turin, 2017.

Tullini P., *Economia digitale e lavoro non-standard*, Labour & Law Issues, 2016, 2(2), 1–15.

Tullini P., *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa, in Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, Turin, 2017, p. 6 ss.

Tullini P., *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro: uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali,* Volume 58 of Treaty on commercial law and public economic law, Cedam, Padua, 2010.

Veliz C., *Privacy is Power*, Penguin Random House, London, 2021.

Veneziani B., *I controlli dell'imprenditore ed il contratto di lavoro*, Cacucci, Bari, 1975.

Voza R., *La tutela del contraente forte nel diritto del lavoro,* in Rivista italiana di Diritto del Lavoro, fasc. 1, 2015, p. 15.

Weiss M., *Digitalizzazione: sfide e prospettive per il diritto del lavoro*, Giuffrè, Milan, 2016.

Woodcock J., Graham M., *The gig economy: A critical introduction*, Polity, Cambridge, 2019.

Zilio Grandi G., Biasi M., *Commentario breve alla riforma "Jobs Act"*, Cedam, Padua, 2016.

# SITOGRAPHY


Article from The Medi Telegraph: *Never in Italy, to amazon and its bracialet*, 2018, in: https://www.themeditelegraph.com/en/transport/intermodal-and-logistics/2018/02/03/news/never-in-italy-to-amazon-and-its-bracelet-1.38085393.

Authorization No. 1/2016, *Authorization to process sensitive data in employment relationships* of December 15, 2016 (published on G. U. No. 303 of December 29, 2016) [doc. web. n. 5800451].

CNBC website: https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html.

D.Leg 10 August 2018, No.101. Full Article on Gazzetta Ufficiale: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true.

Data Protection Supervisor (2018), *Guide to the application of the European Regulation on the protection of personal data*, Luxemburg, Edition update February 2018, p.26-27, in: https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf.

Deloitte, *Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry*, in: https://www2.deloitte.com/content/dam/insights/us/articles/consumer-data-privacy-strategies/DUP_970-Building-consumer-trust_MASTER.pdf, 2014.

Deloitte, *Industry 4.0. Challenges and solutions for the digital transformation and use of exponential technologies,* Zurich, 2015, PDF.

Details of Treaty No.108. Full information: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

Electronic Monitoring & Surveillance Survey, full link: http://www.epolicyinstitute.com/2007-survey.

European Commission, Important answer to the question *When a DPO on personal data is necessary?*, in: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_it#:~:text=È%20necessaria%20una%20valutazione%20d,vasta%20scala%20degli%20spazi%20pubblici.

European Union Agency for Fundamental Rights, Council of Europe, Registry of the European Court of Human Rights, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018.

ILO (International Labour Organization), *Protection of Workers' Personal Data,* in: https://www.ilo.org/legacy/english/intserv/working-papers/wp062/index.html.

L. Manning, *Neoliberalism: what it is, with examples and pros and cons*, in: https://www.investopedia.com/terms/n/neoliberalism.asp, 2022.

PWC EU services on behalf of the European Commission, *Boosting the Potential of Key Enabling, Belgium*, in: https://www.cecimo.eu/wp-content/uploads/2016/03/KETs-skills-brochure_with_CECIMO.pdf, 2016.

Report Digital 2023, *I Dati Globali, We Are Social*, https://wearesocial.com/it/blog/2023/01/digital-2023-i-dati-globali/.

Report McKinsey Global Institute, *Automazione: come cambia il lavoro? Quale impatto su crescita e produttività?* January, 2017.

S. Chiti, *Che differenza c'è tra smart-working e telelavoro*? in: https://www.quindo.it/telelavoro-e-smart-working/, 2021.