HUNGARIAN LABOUR LAW
E - J O U R N A L

The balance in the labour relationship due to Artificial Intelligence and data protection

Chiara Ciccia Romito*

1. Introduction

The world of work is constantly changing. The introduction of artificial intelligence and new technologies in the work environment are changing traditional relationships and affecting the internal balances of this relationship. The use of data is becoming a key element in business strategy because artificial intelligence feeds on it.

A World Economic Forum survey report said that by 2026 corporate governance will have faced a large-scale process of robotization, resulting in human directors sharing their decision-making powers with artificial directors becoming the new norm[1].

Scholars argue that we now live in an online life and there is no turning back[2]. This is now a fact, something that is accepted as the truth, which is being taken up by scholars all over the world to find a new way of regulating relationships between people and AI in the workplace.

At the moment, it is not possible to directly identify this balance as the base of problems that I will explore throughout the paper.

The problems related to the opacity of the algorithms, which could prevent the employer from coming to know the algorithmic codes. Furthermore, it is difficult to understand the logic used by the algorithms deployed in automated decision-making processes. This problem relates to both parties in the labour relationship. The Employers' Associations and Trade Unions could have problems understanding how Artificial Intelligence works.

* PhD Candidate in Labour Development and Innovation, Università degli Studi di Modena e Reggio Emilia, Fondazione Marco Biagi.

1 *Deep Shift – Technology Tipping Points and Societal Impact*. World Economic Forum, Global Agenda Council on the Future of Software & Society, 2015. www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015

2 F. Pasquale: *The black box society.* Harvard Univ. Press, 2015.; Antonio Aloisi – Valerio De Stefano: *Il tuo capo è un algoritmo.* Laterza, 2020.

There is a need for a clear framework relative to the needs at stake, likewise, on the business side. Indeed, the difficulty emerging from algorithmic management also affects the entrepreneurial side, especially the weaker, small and medium-sized enterprises. These are often left out of academic discourses related to algorithmic risks.

2. The risks and reward of AI in the labour market

There are also positive aspects of AI. Artificial intelligence promises to support human well-being, economic prosperity, and sustainable growth. With the advancement in machine learning, there is access to computing power at ever-lower costs, increasing availability of data, and the ubiquity of digital devices. AI is set to benefit the public, private, and third-party sectors. It has become a growing resource of interactive, autonomous, self-learning agencies that can perform tasks that would otherwise require human intelligence and intervention to be successfully executed[3].

Artificial intelligence is becoming an enabling measure for competitiveness, a new need for all types of enterprises including SMEs.[4]

Considering that technological evolution is now irreversible, and that from this comes the need for regulation on a European level, the use of artificial intelligence has caught the attention of scholars and researchers regarding the risks arising from the use of artificial intelligence in the labour market.

Work represents in modern systems a principle of social mobility through which the individual expresses his or her personality[5]. As far as the future is concerned, there are those who speculate on the worst possibility, namely, that work no longer has the present fundamental value and can no longer be an expression of the individual's principle of social mobility[6].

Risks related to personal data and protecting personal data has created a mass corporate surveillance for this type of data, meaning that the free will of workers have been destroyed by surveillance algorithms.

The draft regulation on artificial intelligence considers these two sides of the coin, on the one hand the benefits that could come to the economy in terms of growth and competitiveness, and on the other the risks associated with it.

---

3 Luciano Floridi – Josh Cowls: A unified framework of five principles for AI in society. In: Luciano Floridi (ed.): *Ethics, Governance, and Policies in Artificial Intelligence*. Springer, 2021. 5–17.

4 The proposed regulation on artificial intelligence issued on April 21, 2021, by the European Commission also aims to include SMEs in the regulatory process. As well as accelerating access to markets, including through the removal of barriers for small and medium-sized enterprises (SMEs) and start-ups. Proposal for a Regulation on Artificial Intelligence p. 36. According to the White Paper published by the European Commission, it will also be important to ensure that SMEs can access and use AI. page 30, April 19, 2019.

5 Mortati: *Il lavoro nella Costituzione*, in Enc. Del Dir. Voce Cost. dello Stato, pag. 214.

6 Sussikind: *A world without work*. Metropolitans Books, 2020.

The threat on transparency, however, is not the only risk in the use of artificial intelligence; in fact, if we look at the proposed regulation, we have a list of additional risks identified by Article 15 in which there are risks to systems robustness, cybersecurity, and accuracy. The need to establish a security plan for artificial intelligence systems has also been reiterated by ENISA, the European Cybersecurity Agency, where their latest published document insists on the correlation between the success of intelligent systems and cybersecurity of systems[7] .

The purpose of this paper is to show the side of the coin regarding the risks of artificial intelligence in the labour market[8]. While it is true that the risk of algorithmic opacity is overwhelming and deep learning processes risk breaking the rules of transparency set by the system and implement mass surveillance even beyond the company. These problems are inherent in the very nature of certain artificial intelligence systems, they risk affecting the protection of an employee's personal data and adversely affecting his or her self-determination.

In fact, as subject experts argue, *"in the contemporary world of work, algorithms take the employer's interference – his authority – to a completely different level, equipping it with properties whose nature is located in technology"*[9].

3. The Employee and Employers Interaction with AI

The power of artificial intelligence also affects entrepreneurs who risk facing prejudice in the exercise of their role as employers, but in the simplest theory of making it difficult to exercise their obligations based upon existing regulations.

It is not only the fact that you risk erasing an entrepreneurial class, (we all know the modern idiom of *if your boss is an algorithm*), but also the reference to the fact that algorithmic opacity risks invalidating the awareness of the employer, who, like the employee, is risking staying unaware of algorithmic processes. In this assumption, he or she would be guilty, blamelessly, of hidden, third-party surveillance. Indeed, the expansion of supply chains make surveillance no longer a factor limited within the corporate perimeter; the boundaries of the enterprises are expanded. Thus, the issue of surveillance that can no longer be contained within boundaries, is widened.

---

7 *Cybersecurity of AI and Standardisation*. ENISA, March 2014, available https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation

8 It should be mentioned that current European cybersecurity legislation is changing and moving in the direction of including in certain cybersecurity obligations (which at the time of writing this paper are reserved only for certain types of companies). The NIS 2 Directive intends to include certain medium-sized companies as well. This is certainly a significant finding that demonstrates the need for greater attention to this type of enterprise.

9 M. Otto: A step towards digital self- & co-determination in the context of algorithmic management systems. *Italian Labour Law e-Journal,* Vol. 15, Issue 1. (2022).

Regarding small and medium-sized enterprises, I emphasize that they, in addition to being the subject of a specific population projected by the institutions to invest in smart forms of business, are in danger of the same risks related to algorithmic opacity as larger enterprises.

However, there is also a huge difference between SMEs and large enterprises in terms of privacy compliance in data management, as well as from a trade union perspective.

In fact, the GDPR requires member states to implement simplification measures for small and medium-sized enterprises. Recital 13 recalls the obligation for member states to apply simplification measures to GDPR compliance[10]. The GDPR itself relieves SMEs of certain requirements such as keeping a register of processing activities and appointing a Data Protection Officer[11]. Individual data protection authorities take appropriate measures for simplification. The Italian one, for example, has already provided simplification measures on its institutional website[12].

As far as trade unions are concerned, the Italian Workers' Statute[13] in particular, Title III of the Statute (Articles 19–27) contains several measures to support trade union activity, including the right to establish, at the initiative of workers, company trade union representations (RSAs) in every production unit employing more than 15 employees (Article 35 Workers' Statute).

This is not a small matter considering that there are 25 million SMEs in the European Union, which play a key role in the economy: in fact, they constitute 99% of all enterprises, employ about 100 million people (providing two-thirds of private sector jobs) and generate about 56% of the Union's gross domestic product[14].

As it has been emphasized, the common factor between small and large businesses when it comes to artificial intelligence and data protection is risk, its management and the methodology used to avoid it.

The question arises, whether the current regulatory drafts are effective in avoiding an overlap of bureaucratic acts and can it get to the main purpose: to benefit the economy, job growth and the defense of human ethics.

---

10 In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States.

11 Artt. 30 e 37 of the GDPR.

12 Garante per la protezione dei dati personali, https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

13 Law 300 of 1970.

14 State of the Union of SMEs. European Parliament, giugno 2021. available https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690633/EPRS_ATA(2021)690633_IT.pdf

4. The Current Data Protection Framework for Artificial Intelligence

The digital development of business and the rapid growth of the digitalization in all workplaces and social contexts has led data protection to become an enabler for the adoption of new technological processes.

In European systems, the concept of personal data protection for the purpose of protecting employee privacy has expanded becoming what academics determine to be a privacy 4.0 concept. The concept of 'Privacy 4.0' represents the stages of development of this right. Privacy has moved forward with different 'layers' or 'levels' in its overall scope of protection. This is due to the technological responsiveness of the right to privacy. It gives the right a broader meaning in the employment law and technology debate and makes it relevant in the future of work contexts, sometimes framed in making use of 'Industry 4.0.'[15].

The right to privacy can be seen as one of the gateways for human rights protection in the data economy. A violation of privacy can impact other human rights[16].

This reason, among others, has resulted in more severe penalties being given for breaching privacy regulations set by the current framework.

In this section, we will analyze the current regulatory framework on data protection and artificial intelligence. In particular, the measures that the employer must take within the current regulatory environment.

The first article is Article 22 of the GDPR, which recognises the data subject's right not to be subjected to automated decision-making processes, including profiling.

For the purposes of application, it is, therefore, necessary that the decision, which is based solely on automated processing of personal data, influences the legal sphere of the data subject, or affects the person in a significant or similar way.

This right, however, found in paragraph 2 below specifies exceptions; paragraph 1 not being applicable when automated decision-making: a) is necessary for the conclusion or requirement of a contract between the data subject and a data controller; b) is authorized by the law of the Union or the Member State to which the data controller is the subject; c) is based on the explicit consent of the data subject.

The hypothesis that can be traced back to the employment relationship is the contractual one referred to in (a), since it is now accepted that consent is not, in the context of employment relationships, a suitable legal basis by virtue of the imbalance of powers between the parties[17].

---

15 F. Hendrickx: *Privacy 4.0 at work: regulating employment, technology and automation*, 2019.

16 Isabel Ebert – I. Wildhaber – J. Adams-Prassl: Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection. *Big Data & Society,* Vol. 8, Iss. 1. 2021.

17 The relationship of subordination in employment is distinguished by being a non-"equal" relationship. According to Article 4 para. 11 of the GDPR, consent is formed by any manifestation of the data subject's free, specific, informed and unambiguous will, by which the data subject indicates his or her assent, by means of an unambiguous affirmative statement or action, that personal data

Paragraph 3 of Article 22, in the hypothesis of (a) and (c) above, establishes an additional obligation to provide safeguards for the data subject: in fact, the data controller appears to be obliged to implement appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, and at least the right to obtain human intervention of the data controller, to express his or her opinion and to contest the decision. To do this, the data subject must be put in a position that encourages knowledge about the automated data processing that concerns him or her. It is, therefore, essential to comply with the requirements of Article 13 of the GDPR, which, in paragraph 2 (f), explicitly recalls the obligation to communicate to the data subject's meaningful information about the logic used, as well as the importance and expected consequences of such processing for the data subject. This is complemented by Recital 59, which states that it is appropriate for the data controller to facilitate the data subject's exercise of the right to access. Recital 71 complements the already mentioned rights with that of obtaining a specific explanation of the decision made by automated decision-making.

Article 15 of the GDPR grants the data subject the right of access to personal data of themselves, that has been processed by the controller, retells the provisions of Article 13, reaffirming the data subject's right to access such information.

Systematic reading of the articles has led some of the doctrine to define the set of guarantees as the "right to legibility" of the data and algorithms involved in automated decision making[18] .

However, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 clarified that the data subject's right to know about the processes of personal data concerning him or her pertains only to the logic used and not necessarily to a complex explanation of the algorithms used or disclosure of the full algorithm[19].

Having defined the boundaries dictated by the GDPR, it is consequently necessary for how the data subject can exercise his or her rights especially in the employment context.

In the first instance, it appears necessary to investigate the effectiveness of the protection provided by the GDPR about the main issue related to the opacity of the algorithm. The issue related to the "explainability" of the algorithm gains more relevance in the labour market for two main reasons. The first reason is related to the trade secret of which the intelligent system's source codes might possess. Moreover, the entrepreneur himself might not be aware of this, due to the intrinsic structure of the algorithm because of the trade secret.

concerning him or her be processed. The employer's interference could, even indirectly, affect the employee's freedom of choice by vitiating, therefore, the validity of the consent. Precisely by virtuè of these reasons, even the Article 29 Working Party in its Opinion 2/2017 on the Processing of Personal Data in the Context of Labour Relations stated that it is highly unlikely that consent constitutes a legal basis for the processing of data in the workplace.

18 Gianclaudio Malgieri – Giovanni Comandè: Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. *International Data Privacy Law,* Vol. 7, Iss. 4. 2017.

19 Article 29 Data Protection Working Party, https://ec.europa.eu/newsroom/article29/items/612053

Such an eventuality could result in the impossibility of fulfilling the employee's right to transparency, and personal data could be processed in a manner completely hidden from the employee. This could lead to employer liability and problems with employment practices and privacy obligations.

The second reason, on the other hand, relates to the very nature of A.I., as reiterated in the opening of this paper i.e., the difficulty of obtaining the explanation of the logic used due to the complexity of the intelligent systems themselves.

The use of complex systems and deep learning, which exploits complex systems (hence also the term black boxes[20]), could prevent workers from exercising their rights by default.

Additionally, assuming that from the intelligent software we can derive the logic used under Articles 13, 15 and 22 of the GDPR – are we certain that the worker has the technological capabilities to understand it? This verification is also necessary about the employer – are we certain that the contractor has the capabilities that the legislation gives him.

To this extent, the question arises as to whether union representatives today have, in turn, sufficient knowledge to assist the worker in the exercise of these rights, or whether the identification of specialized figures aimed at translating the "smart" language to the totality of the corporate population is necessary. Such an eventuality especially arises with reference to the SME category, where the union component is mostly absent. The problem of transparency also arises with reference to the implementation of the protection provided for surveillance that results from the use of intelligent systems.

In Italy, the norm provides different forms of protection to the instrument used by the employer. In the first paragraph, for instruments from which monitoring of the workers could be a result, the rule conditions processing operations and monitoring by the employer on the existence of specific legitimizations and prior union agreement or, failing that, administrative authorization. In the second paragraph, it regulates hypotheses related to the use of work tools necessary to render work performance: in these cases, the rule does not require the implementation of the guarantees set forth in the first paragraph of Article 4 of the Italian Workers' Statute.

As noted already in the opening of this paper the expansion of active contributing stakeholders in the operation of intelligent systems remains another lingering matter. Stakeholders as A.I. providers could become aware of the personal data of workers processed by the enterprise, so that monitoring of workers would extend beyond the company parameters.

The question arises about the safeguards offered by the current legislation and whether they are sufficient in hypotheses – such as those envisaged – where surveillance may be exercised not only without the employer's knowledge, but by outsiders[21].

---

20 F. Pasquale: *The black box society. The secret algorithms that control money and information*. Cambridge, Harvard University Press, 2015.

21 Karen Levy – Solon Barocas: Refractive Surveillance: Monitoring Customers to Manage Workers. *International Journal of Communication,* Vol. 12, 2018.

These issues also apply to the entrepreneurial side not only to workers but also employers because they may also lack the skills to understand algorithmic logic. Is the party placed to protect the entrepreneurs, namely the business associations, capable of supporting the employer in this new technological environment?

This issue is even more vivid in SMEs that lack the appropriate organization to handle the bureaucratic burden that could result from the use of intelligent systems as well as the skills to understand the technology.

With all the above being said, it can be concluded that the GDPR is, therefore, the main useful tool for creating awareness of data protection. Moreover, the provision of Article 25 and the principle of privacy by design together with what is recognition under Articles 15 and 22 of the GDPR could avoid the problems arising from algorithmic opacity. However, they seem like abstract predictions that when dropped into reality struggle to find recognition. From the understanding of the logic used to address the issues so far related to employers, risk contributing to a difficulty in the exercise of rights and an aggravation of responsibilities for employers.

This problem is especially found within smaller business contexts where the organization by structure and simplified measures is impossible for the exact fulfillment of the obligations and rights recognized by it.

5. The draft Regulation on Artificial Intelligence

On April 21st 2021, the European Commission published the Proposal for a European Regulation establishing harmonised rules on Artificial Intelligence. The Proposal follows numerous initiatives and publications setting out the principles and values Europe wants to comply with when using A.I.[22].

Indeed, there are numerous references to papers issued in recent years in which the European institutions have focused attention on various aspects arising from the application of A.I. In particular, on the ethical implications and the protection of individual rights. The shared objective of the papers is the creation of user trust within A.I. systems. This objective can be achieved following the establishment of a robust European approach capable of defining the regulation of A.I. and the safeguards necessary to protect people's rights against the risks that may arise from the implementation of the new "intelligent" systems in the same manner in all Member States.

In order to achieve the above-mentioned objectives, the Commission has developed a risk-based approach based on the degree of risk (unacceptable, high risk, all other cases). In addition, the reliability of the system and the adoption of a two-step alternating enforcement mechanism.

22 See *Excellence and Trust in Artificial Intelligence 2020; White Paper on Artificial Intelligence: A European approach to excellence and trust 2020; Proposal for a Regulation on machinery products 2021.* Available on the institutional website of the European Commission.

One before the product is placed on the market and one after, aimed at monitoring compliance of the product placed on the market. The acceptability or otherwise of the risk is determined by the implication that the A.I. system might have on the rights of the individual; to this end the Commission lists in Annex III of the Proposal the systems that may not may not be placed on the market[23].

The classification of an A.I. system as high-risk is based on the intended purpose, in line with existing EU product safety legislation. Consequently, high-risk classification depends not only on the function performed by the A.I. system, but also on the specific purpose and manner of use of that system. Chapter I of Title III lays down the classification rules and identifies two main categories of high-risk systems. High risk systems that are intended for use as safety components of products subject to *ex ante* conformity assessment by third parties and stand-alone. High systems that have implications primarily in relation to the fundamental rights explicitly listed in Annex III of the Proposal[24]. In order to successfully implement A.I. systems in the market, the Commission provides reinforced monitoring and evaluation mechanisms with the provision of public registers and reporting processes to the authorities in the event of serious incidents or malfunctions.

The proposal also devotes particular attention to the principle of transparency, which, as already stated, constitutes an enabling element in the protection of personal data of natural persons.

Firstly, it can be seen that the scope of the proposal is strictly limited to certifying the product before it is introduced into the market. Nothing is foreseen for the subsequent phase and after the product has been introduced into the working environment. These provisions seem to be mainly in the hands of the Member States.

The all-inclusive approach of the proposed regulation does not differentiate the sectors of application, a high risk is equally identified in the education sector as in the employment sector. The common denominator represented by high risk, which is independent of the sector of application, does not offer the specific protections based on the sectors in which the A.I. system may be applied to and from which derive different consequences, each deserving protection.

While providing some necessary guarantees for market entry, the proposal does not seem to be able to guarantee the specific necessities to protect the delicate interests at hand. Especially in those contexts, such as the workplace, where the dignity of the person needs protection.

Therefore, the problems highlighted above remain present, because right now the proposal is not able to eliminate issues related to deep learning, data access, and at least issues related to the comprehensibility of new business processes.

---

23 This category includes the use of A.I. by public authorities for the purpose of obtaining so-called "social scoring" for assessing the behaviors of individuals, the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes (subject to certain exceptions), and subliminal techniques aimed at significantly altering a person's behaviors in a harmful way.

24 *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence and amending certain legislative assets of the Union*. Brussels,2021.

6. Is balance possible?

Analyzing the outlines of the current regulatory framework and issues related to the use of artificial intelligence, it seems clear that one consequence could be that of the burdening of obligations and an increase in employers' liability. Strategic litigation has partially revealed the responsibility of employers in terms of window-dressing internal operations under the veneer of seemingly inexplicable "black boxes" that penalize certain groups of workers[25].

In some cases, the code changes after a decision has been made: a full reconstruction of the inner working is not a simple task. On the contrary, the implied "uncertainty principle" should prompt workers and litigants to rely on evidentiary instruments that leverage the lack of shared information to boost the claimant's attempts to overcome such "fogginess[26]". This has led academics to argue that the burden of proof should be shifted to the employer, leading to an additional burden of obligations in terms of algorithmic risk management. The framework leads one to reflect on the status of the employer on its responsibilities and what the balance is in the future world of work. The ideas emphasized by Adams-Prassl reveal the concept of employer has been neglected in both judicial and academic discussions or occasionally considered residually from a purely contractual perspective[27]. This element increases in relation to the new forms of smart work, which, as explained above, weighs down the burden of obligations on the employer. This issue increases in magnitude with reference to SMEs, who are in danger of being weighed down by the challenges of understanding and addressing regulations in the area, while also trying remain competitive. Here, SMEs face a significant resources (human and financial) issues as compared to large companies. In addition, there has been a significant shift from centralized decision-making to scattered and outsourced power centers[28].

There is a clear need for legal regulation to ensure that emerging technologies are deployed within the proper boundaries. Over the past few years, the legal challenges arising from 'big data' and machine learning have increasingly become the focus of extensive academic discussion, both in computer science and more traditional legal debates. At the same time, it is not always clear whether the ideas proposed could work in the very specific regulatory context of employment law. Given the specifics of the personal employment relationship, solutions proposed in general contexts, or even other areas such as consumer protection, cannot necessarily be translated across. This point can be illustrated briefly by reference to the three areas explored in the preceding section[29].

---

25 Antonio Aloisi: Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights. *International Journal of Comparative Labour Law and Industrial Relations,* 2022.

26 Giovanni Gaudio: Algorithmic bosses can't lie! How to foster transparency and limit abuses of the new algorithmic managers., *Comparative Labour Law & Policy Journal,* 2021.

27 Jeremias Adams-Prassl: *The Concept of the Employer.* Oxford, Oxford University Press, 2015.

28 Levy–Barocas op. cit.

29 Jeremias Adams-Prassl: What if your boss was an algorithm? *Comparative Labour Law & Policy Journal, 2019.*

Scholars in the sector, that I have already mentioned, suggest that the current European regulatory plan is unable to address the individual challenges associated with the introduction of the world of artificial intelligence. In particular, Technological transformation is a multidimensional phenomenon, the constituent elements of which (as well as the interests related to them) are so closely intertwined so that consequences of any specific regulatory intervention will almost always exceed its original scope and purpose, and in this regard, it is worth noting that the impact of technological transformation does not only concern the development of new policies and new regulatory instruments but it also extends the need to review existing categories to understand the purpose of proper management of new forms of work[30].

In this framework, subject to all the risks related to workers that are not questioned and remain the main issue. We need to turn our attention to the status of the entrepreneurs and understand the risks regarding the algorithmic opacity that could affect the organization and the bureaucratic burden that could invalidate the business continuity of the enterprise. As repeatedly mentioned, this need is more urgent for SMEs because they lack interaction with trade unions and on the other hand because they are different in organization.

If one tries to identify possible solutions or conclusions to this issue, three main issues emerge: the first is related to the very nature of artificial intelligence, which with its complexity risks being incomprehensible to the employer who may be unable to properly implement what is enshrined in Articles 15 and 22 of the GDPR. Doing so would risk undermining the right of access and the multi-step transparency called for in the data protection legislation, which as is well known to make transparency the main point for building trust.

When we talk about data protection and transparency, in the view of technological development we must consider transparency as a social benefit. Personal data protection, Rodotà wrote, thus began to walk with two legs: confidentiality and control. To the first was suited silence. To the second, transparency[31].

Secondly, there should be in the hopes – for hypothesis that the problems related to algorithmic opacity are resolved there remains the problem of understanding whether access to the logic used and to challenge the decision recognized by Articles 15 and 22 of the GDPR is an exercise that can be implemented especially within unstructured business contexts without union representation. However, it is necessary to investigate the actual ability of the parties to understand the content of the so-called rationale used. Against this backdrop, the latest issue moved by the need to regulate artificial intelligence in the labour market at the domestic, not just European, level.

---

30 Iacopo Senatori: EU Law and digitalisation of Employment Relations. In: Tamás Gyulavári – Emanuele Menegatti (eds.): *Decent work in the digital age: European and comparative perspectives.* Hart, 2022.

31 Giovanni Ziccardi: *Diritti digitali*. Raffaelo Cortina Editore, 2022. 50.

There is a need to investigate the role of unions closest to workers, such as representatives, and associations representing businesses to understand what part they play in this new market revolution and enterprise risk management.

Once these answers are identified, it will be possible to try to outline a balance between workers' rights and employer responsibilities. For now, the power of artificial intelligence does not exempt anyone even the party that has so far always been considered strong.