Protection Against the Risks and Abuses of Algorithmic Management in the European Legal System: The Need for an Integrated Approach

Pia De Petris

University of Milan, Milan, Italy

The essay, after analysing the risks of algorithmic management to workers' fundamental rights, examines the protections available within the European legal framework. It provides an integrated analysis of three regulatory areas that can be invoked against algorithmic opacity: data protection, anti-discrimination laws, and algorithmic transparency. This integrated approach leads to the conclusion that European social law offers important tools to counteract abuses of algorithmic power. However, there are areas of uncertainty which must be addressed by general recognition of the rights to algorithmic transparency, explicability, and understanding which must be granted to workers and their representatives.

Keywords: algorithmic management, artificial intelligence, risks, safeguards, European regulation, integrated approach

The Algorithmic Management: Opacity and Risks to Workers' Fundamental Rights

The use of algorithmic technologies and artificial intelligence (AI) in organizational management and human resources (a phenomenon now known as "automated" or "algorithmic" management) presents labour law with complex regulatory challenges. These tools have the potential to significantly impact employment relationships and transform traditional methods of exercising managerial authority (Aloisi, 2024; Pizzoferrato, 2021; Gaudio, 2023; Prassl, 2022).

Algorithmic management involves shifting traditional organizational and managerial tasks from human staff to intelligent machines. These machines, as an expression of a more rapid, accurate, and objective form of management than human oversight, promise to enhance the efficiency, productivity, and competitiveness of the digitalized enterprise, creating the most pervasive and systematic integration of technology into business activities. The organizational change underlying this shift is characterized by depersonalization: Algorithms are entrusted with—or perhaps more appropriately, delegated—some of the prerogatives that are typically assigned to the employer and the client, or otherwise left to managers: assign tasks, give instructions, monitor and assess the work performed, provide incentives, or impose penalties.

Pia De Petris, Ph.D., research fellow, Department of Labour Law, University of Milan, Milan, Italy.

The area where algorithmic management is most extensively tested is undoubtedly digital platform work, where sophisticated algorithms are capable of managing, almost entirely, the organization of work (Santucci, 2024; Prassl, 2018; Carinci & Dorssemont, 2021; Perulli & Bellomo 2021). Recently, however, in Europe, automated management systems are also spreading to more traditional sectors, such as logistics and services (for example, in the case of wearable devices, on which see Kelly-Lyth & Thomas, 2023), even gaining ground in the public sphere, in the process of forming administrative measures and judicial decisions (Biasi, 2024).

Algorithmic management responds to new forms of rationality and creates an unusual blur between the "algorithmic code" and the "legal code", which risks narrowing the scope of traditional regulatory intervention. This situation requires new approaches to power dynamics, aligned with the operational logic of algorithms and the new challenges they pose.

Regarding the use of such systems, one of the greatest risks for the protection of individuals subjected to automated systems is the difficulty of interacting with the "machine" and reconstructing its exact functioning ex post, and thus understanding the impact it has on their working conditions (the so-called issue of algorithmic opacity, on which see Burrell, 2016).

This difficulty, when applied to the workplace context, risks further exacerbating the informational asymmetry and power imbalance that characterize the employment relationship.

Employer power in algorithmic management is managed through devices, software, and multifunctional digital applications that serve as both work and control tools, enabling continuous and uninterrupted supervision (Aloisi & Gramano, 2019).

This creates an organizational scenario in which the employer, through the "omnipresent" algorithm, strengthens their prerogatives at the expense of workers, who, if poorly informed about the functioning and impact of algorithmic management, find themselves unable to recognize the biases they face, or are disadvantaged in acquiring sufficient evidence to assert their rights in court (Otto, 2019; Kinowska & Sienkiewicz, 2023).

It is clear, then, that the issue of algorithmic opacity can be considered a sort of "meta-risk" since, without decoding the functioning of the algorithmic machine, it is difficult to prevent and monitor other potential risks arising from the use of such systems: privacy violations, discrimination, breaches of the limits on control and disciplinary power, and so on.

To address this "meta-risk", it is essential to understand the root cause of the issue of algorithmic opacity.

Undoubtedly, at the heart of the issue are technical reasons related to the functioning of certain technologies, but at the same time, there are also legal reasons, related to the need to adapt and update protective measures in response to the reality of the algorithmic and/or digitally integrated enterprise.

In particular, it is important to consider that there are different types of algorithms, which can be grouped into two main categories: rule-based (RL) and machine learning (ML) algorithms. In the first case, the machine's decision-making process is static and deterministic: To solve the class of problems presented, the algorithm follows the rules set in its programming, with an inductive calculation process that produces results that are predictable beforehand. Machine learning (ML) algorithms, on the other hand, are characterized by higher levels of complexity. Their functioning depends on the extensive collection and processing of large amounts of data, from which the machine can learn patterns of "action", "decision", and "behaviour" (Shalev-Shwartz & Ben-David, 2014).

It follows that the computational process of these algorithms is dynamic and deductive, based on statistical and probabilistic relationships. In these cases, the algorithm, through the statistical management of accessible data, learns in a conditioned manner based on external interactions it encounters, making predictions and thus arriving at results that are not predictable in advance.

Moreover, in the field of ML algorithms, deep learning algorithms are in an advanced stage of experimentation. Their functioning, designed to mimic that of neural networks, is based on progressive and autonomous learning from data (with a sort of extraction of deep layers of knowledge through data training). This layered learning, carried out autonomously, makes it difficult to explain each logical step taken by the machine afterward and could lead to irrational outcomes (Peruzzi, 2023, p. 20).

The advent of artificial intelligence technologies has further complicated this scenario (Ponce Del Castillo, 2024; Cefaliello & Kullmann, 2022; Lane & Saint-Martin, 2023; Waas, 2022).

Artificial intelligence leverages computational mechanisms capable of processing novel inference criteria from data. It makes efficient decisions based on this analysis. From the inputs it receives, it generates outputs such as predictions, content, recommendations, or decisions. These outputs hold the potential to influence both physical and virtual environments (Article 3 of Regulation No. 2024/1689 of June 13, 2024—"AI Act"). So, with the advent of AI, it has become even more difficult to identify, after the decision-making process, the factors and variables on which the automated decision was based, as well as the precise weight of each factor in the decision itself (Cristofolini, 2024, p. 75). Considering this reality, it is clear that protective measures need to be rethought from a more proactive approach, aimed at minimizing the risks of uncontrolled, distorted, or discriminatory effects caused by the use of digital automation in the workplace from the outset.

Algorithmic rationalities call for a more proactive regulatory approach, of a precautionary nature, axiomatically oriented towards the primacy of humans over technology. This approach seems to be gaining ground in recent European regulatory actions, which have sought new tools to strike a balance between supporting digitalization and protecting fundamental human rights.

The European Approach to the Risks of Automated Management: A Mapping of the Sources of Law

As anticipated, in the era of automation and AI, the essential challenge for labour law is to adapt the framework of protections to new work organizations, seeking to limit and neutralize the risks associated with the exercise of unchecked and opaque power.

This challenge has been at the core of the European regulatory agenda in recent years, which has become a global leader in regulating the latest technological frontiers, ushering in a new phase of the European regulatory approach, which some have termed the "New European Digital Constitutionalism" (De Stefano, 2022; Senatori, 2020).

One of the initial regulatory initiatives in this field is the White Paper on Artificial Intelligence, launched by the European Commission in February 2020. This document, which outlines the European regulatory plans for the AI sector, identifies seven foundational requirements for the development of AI systems: (1) human oversight and intervention; (2) technical robustness and safety; (3) privacy and data governance; (4) transparency; (5) diversity, non-discrimination, and fairness; (6) social and environmental well-being; and (7) accountability.

These value-based requirements were subsequently articulated, albeit with varying emphasis, across a range of distinct regulatory acts adopted for different (but often complementary) purposes. This compartmentalized regulatory approach does not facilitate the work of legal practitioners and may prove less effective than a single, integrated regulatory framework (e.g., a protective statute for individuals working in the AI era).

Nevertheless, despite the numerous and diverse European regulatory measures, it is still possible to discern a coherence in the regulatory approach, which, on an axiological level, is grounded in the anthropocentric principle ("human in command" and "human in-the-loop"); on the legal technicality level, it instead relies on the modulation of protections based on the level of risk (risk-based approach as noted by Gellert, 2020), according to the principles of precaution and prevention, as a safeguard of fundamental rights (Aloisi & De Stefano, 2023; Adams-Prassl et al., 2023).

This approach is, for example, generally pursued regarding the European regulation of the online platform market, through two complementary regulations adopted in 2022: the Digital Markets Act and Digital Services Act, which have horizontally reinforced some of the protections already established for commercial users by Regulation No. 2019/1150/EU. Both regulations, adopted to curb the concentration of market power in the hands of big online platform companies, respond (as does Regulation No. 2019/1150/EU) to a preventive regulatory approach, based on risk (De Gregorio & Dunn, 2022): They foresee, under the banner of accountability, a series of preventive procedural guarantees, concerning duties of transparency, disclosure, monitoring, and risk analysis, regarding the activities of intermediary or informational platforms, especially those related to the management of users' personal data, effectively revitalizing the approach already introduced with the GDPR.

The risk-based regulatory approach is then elevated as the driving force of the Artificial Intelligence Regulation and the protection of algorithmic transparency as outlined in the "Platforms" Directive (Directive No. 2024/2831/EU), guiding several guarantees already established in the legal framework, which can be invoked as safeguards against the abuse of algorithmic power, such as data protection and anti-discrimination measures (Peruzzi, 2023).

In particular, the AI Act absolutely prohibits the use of certain tools deemed to pose an excessively high risk to fundamental rights. According to Article 5 of the AI Act (which takes effect six months after the Regulation's entry into force), systems involving gamification (Hammedi, Leclercq, Poncin, & Alkire (N é Nasr), 2021), social scoring and emotion recognition (Durovic & Corno, 2024) in the workplace are prohibited, except for systems that recognize physical states introduced for health and safety purposes.

Conversely, for systems that pose a high risk to fundamental rights—including those applied in the workplace—the Article 6 of the AI Act imposes several obligations on both providers and deployers: Providers must conduct verification, risk mapping, implement a risk management system, and train users; employers, as users in the employment context, are responsible for ensuring transparency, providing both individual and collective notifications, monitoring, and explaining the decision-making processes that impact fundamental rights (Cristofolini, 2024, p. 79).

Indeed, although there is no unified regulatory framework in European law (which is certainly desirable, as noted by De Stefano & Wouters, 2022) for the algorithmic management of labour relations, European legislation is nonetheless dotted with regulatory segments that can be invoked to counter the risk of algorithmic opacity (Prassl, 2022, p. 35).

Alongside the general and provisions of the AI Act, three fundamental regulatory safeguards can be identified: (a) data protection; (b) anti-discrimination protection; (c) algorithmic transparency and explainability.

Regulatory Systems Against Algorithmic Opacity: Data Protection

The functioning of AI and automated management systems relies on the management and analysis of large amounts of data. To prevent the risk of algorithmic opacity, data protection is essential, serving as a primary shield against invasive monitoring and data processing practices that undermine the freedom and dignity of workers (Abraha, 2023, p. 180; Prassl, 2022, p. 30).

In European privacy legislation, there are significant principles and rules to protect both self-employed and employed workers subject to algorithmic management.

The European General Data Protection Regulation No. 679/2016 (GDPR), directly applicable in EU member states, including in private relationships (and thus in employment relationships), aims to hold companies accountable in preventing risks to fundamental rights such as freedom, dignity, and self-determination (Ingrao, 2022, p. 130), following a risk-based preventive regulatory model, whose strategic importance has already been emphasized in the context of algorithmic management.

In fact, the GDPR requires companies to adopt appropriate legal and technical-organizational measures to safeguard personal data, ensure transparency, and maintain fairness in data processing, in compliance with the principles of purpose limitation, transparency, and minimization. This is achieved through an approach that incorporates protection by default, known as privacy by design and privacy by default (Art. 25 GDPR). In order to uphold these principles, the GDPR gives data subjects specific rights to prior information (Art. 13 GDPR) and rights to access data being processed (Art. 15 GDPR).

The GDPR specifically addresses automated processing in Article 22: The first paragraph recognizes "the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning him or her, or significantly affects his or her person".

In a recent ruling, the Court of Justice clarified that the "decision" referred to in Article 22 should not be understood in a narrow sense as a formal decision but can also encompass "measures or assessments concerning personal aspects of individuals", providing a functional definition focused on the impact such measures have on the personal sphere of the data subjects (CGUE 7 December 2023 C634/21, SHUFA Holding AG).

In the second paragraph, Article 22, Letter (a), excludes the application of this principle in cases where the data subject has given their consent and in situations where automated processing is necessary for the conclusion or performance of a contract between the data subject and a data controller. Nonetheless, the general principle remains worthy of protection. This is because, in any case, in the third paragraph, Article 22 provides, in accordance with the anthropocentric perspective ("human in control principle"), the obligation to adopt appropriate measures to safeguard the "right to obtain human intervention from the data controller, to express one's opinion, and to contest the decision". Therefore, even when authorized, automated processing must still be subject to measures that protect the rights, freedoms, and legitimate interests of the data subject, at the very least by guaranteeing the right to express one's opinion, contest the decision made by the algorithm, and request and obtain human review (Tosoni, 2021).

Finally, from the perspective of accountability and risk prevention and management, Article 35 of the GDPR, to ensure the effective implementation of the aforementioned provisions, requires a Data Protection Impact Assessment (DPIA) to be carried out by the data controller (Peruzzi, 2023).

In conclusion, it can be asserted that the data protection regulatory framework provides important safeguards, which, at the outset, require aligning the informational universe underlying the functioning of the algorithm with criteria of transparency, accuracy, precision, data minimization, and so on; moreover, it recognizes the worker's right to be informed about the existence of automated processing, to understand the functioning and influence of such processing on their legal sphere, as well as the right to human intervention for correction.

However, all these safeguards could lose their effectiveness in the face of opaque and difficult-to-interpret algorithmic systems. Consider the principles of purpose limitation, accuracy, adequacy, relevance of processing, and data minimization, which are central to the GDPR: Their practical applicability could be weakened in systems equipped with self-learning capabilities, where the objectives and goals to be achieved are not necessarily predefined, as these systems have the ability to replace the usual cause-and-effect sequence with a opaquer and freer correlation between a multitude of variables. This can lead to the possibility of unexpected outcomes.

Furthermore, even simpler systems are characterized by a continuous capacity for evolution and updating, making it more difficult to control compliance with the requirements of fairness and authenticity in data collection.

It then becomes necessary to reflect, following the integrated approach outlined earlier, on the contribution of other regulatory segments involved, to assess whether these can overcome such limitations.

Anti-discrimination Protection

Another regulatory tool that can be invoked to address algorithmic opacity is anti-discrimination law. In the European legal landscape, anti-discrimination protection was the first legal "tool" employed to open the "black boxes" (Pasquale, 2015) of management algorithms and to assess whether and how automated management might result in abuses or violations of fundamental rights for platform workers involved in automated decision-making processes.

Regarding the issue of discrimination, the introduction of automated systems can have ambivalent effects: On the one hand, it may lead to more rational, objective, and even fairer decisions, as they are free from human errors, biases, and prejudices; on the other hand, however, as argued in academic literature and supported by case law, these systems may also create new and more insidious channels for spreading discrimination. When embedded within opaque and even less transparent mechanisms, discrimination becomes harder to prevent, identify, control, and, consequently, to sanction (Santagata De Castro, 2021; De Simone, 2022; Gaudio, 2024; De Petris, 2024).

Indeed, given the functioning of algorithmic management, the mere introduction of a single distorted data point, parameter or criterion within the vast array of inputs can trigger an uncontrollable spiral of bias propagation. This may ultimately affect the algorithm's final decision, thereby perpetuating a risk of structural and systemic discrimination.

Consider, for example, the case of Amazon's recruiting algorithm. This algorithm was designed to manage candidate screening during the hiring phase, but it systematically excluded female applicants' résumés. The algorithm had been programmed to consider the outcomes of previous hiring rounds, which were characterized by a low representation of women. Consequently, in its effort to replicate past hiring results, the algorithm "learned" to penalize female profiles, thereby resulting in prohibited discrimination (Dastin, 2018).

Even more telling is the Italian case of the algorithms used by Deliveroo and Glovo. These algorithms, programmed to rank riders based on availability and punctuality, discriminated against workers who, due to strikes, illness, disability, religious obligations, or family needs, were absent more frequently and unable to meet the rigid attendance standards imposed by the algorithm (Court of Bologna 31 December 2020; Court of Palermo 17 November 2023, on which see De Petris, 2024).

In response to the new risks of algorithmic discrimination, traditional anti-discrimination law—originally designed to address human discrimination—has proven effective in tackling this frontier of discrimination as well (Kelly-Lyth, 2023; Santagata De Castro, 2021).

Indeed, algorithmic discrimination does not alter the structure of the discriminatory offense, nor does it undermine the established concepts of direct and indirect discrimination. The fact that discrimination occurs unconsciously, through an impersonal automated tool, and even without human intervention, is not determinative under anti-discrimination law. Rather, the concept of discrimination—whether direct or indirect—is objective in nature, as it targets the discriminatory effect, not the intent. Moreover, this protection applies even in cases where discriminatory harm is merely potential and even where specific victims of discrimination cannot be clearly identified, as in cases of collective discrimination.

Therefore, since the concept of discrimination does not require any intentionality, it cannot be ruled out that algorithmic discrimination may also constitute direct discrimination (Prassl et al., 2023). As is well known, direct discrimination is subject to broader protections, leaving no room for justifications, unlike indirect discrimination, which occurs when an apparently neutral criterion or practice has a disproportionately adverse effect on members of a protected category. Additionally, anti-discrimination protection applies even when the disparity in treatment is only potential and even when no specific victim of discrimination can be identified, as in the case of collective discrimination. This protection is further reinforced by granting the judge extensive investigative powers. Once discrimination is established, the judge may order the company, in consultation with labour unions, to implement a plan to remedy the effects of the identified discriminatory practices and to conduct an impact assessment of the tools through which discrimination emerged.

However, it is also true that algorithmic discrimination may be harder to detect, especially when it takes the form of "proxy discrimination", where the discriminatory effect occurs through an indirect reference that is nonetheless correlated with membership in a protected category.

In such cases, the discriminatory potential may be even more obscured, although European anti-discrimination law provides an easing of the evidentiary burden in favour of the victim of discrimination. The risk of algorithmic opacity affects the recognizability of discriminatory treatment, making it more difficult for the workers to offer of evidence of the discrimination suffered due to the algorithmic rule, which is difficult to decode.

Therefore, a central issue remains the need for reflection on the transparency of new algorithmic tools used in the workplace.

Algorithmic Transparency as a Preliminary Safeguard Against Algorithmic Opacity: The Directive No. 2024/2831/EU on Platform Work

Recent European regulatory measures recognize "algorithmic transparency" as an essential tool for protecting against the opacity and inaccessibility of algorithmic and AI systems implemented or applicable in the workplace (Zappalà, 2023, p. 623).

In general, informational transparency, as a cognitive tool aimed at rebalancing the contractual vulnerability of the worker (Zilli, 2022, p. 109), has long been pursued within the European legal framework, beginning with Directive No. 91/533/EEC, which was implemented in our legal system through Legislative Decree No. 152 of May 26, 1997.

More recently, the protection of transparency in employment relations has been revitalized by Directive No. 2019/1152/EU, which, in response to the specific protection needs of new forms of atypical work (especially within the digital context), has the merit of complementing the promotion of informational transparency with that of predictability and security of working conditions. To this end, it establishes certain "minimum requirements" on these matters (Georgiou, 2022, p. 193; Bednarowicz, 2019, pp. 604-623). In the new Directive, transparency serves not only as a tool for rebalancing information but also to uphold the "minimum rights" of work security and predictability. These rights are introduced by the Directive to protect both subordinate workers and falsely self-employed individuals.

The Directive No. 2019/1152/EU, albeit following a "minimum harmonization" model within an essentially binary framework (characteristic, moreover, of European social legislation: see Gramano, 2021), reaffirms transparency as a protective measure aimed at improving working conditions. It functions as a tool to enable various forms of oversight, such as verifying corporate remuneration policies and the potential presence of gender-based discrimination.

The importance of transparency as a protective tool is emphasized by the latest European legislative initiatives, which identify the "algorithmic transparency" as a new regulatory pillar for managing and limiting employer power mediated by algorithms, thereby strengthening the effectiveness of existing regulatory mechanisms. In particular, the protection of algorithmic transparency is pursued through the Platform Work Directive (Directive No. 2024/2831/EU), recently adopted by the European Parliament and Council following a lengthy mediation process on the Directive Proposal of December 9, 2021, No. 762 (Rosin, 2022; Smorto & Donini, 2024; Giovannone, 2024, p. 500).

To ensure better working conditions in platform work, the new Directive grants important transparency rights, as regulated in Chapter III of Directive No. 2024/2831/EU, particularly in cases involving:

(a) "automated monitoring systems", where algorithms are used to monitor, manage, and evaluate the performance of work activities;

(b) "automated decision-making systems", where algorithms are used to make or support decisions that affect working conditions and employment relationships.

In both cases, the Directive specifies that these systems have a "significant impact on working conditions" and pose a "high risk to the rights and freedoms of natural persons" (Article 8).

To minimize these risks—a goal already pursued broadly under the AI Act—Article 7 of the Directive strictly prohibits the processing of personal data that are not directly relevant and necessary for fulfilling the employment contract (e.g., data from private conversations or sensitive data, including biometric, health-related, emotional, or psychological data, as well as data related to the exercise of fundamental rights, especially union membership and the right to strike).

Furthermore, in line with the principles of "human-in-command" and risk management, Article 8 of the Directive requires digital labour platforms to conduct data protection impact assessments, as outlined in Article 35 of the GDPR, with prior consultation of platform workers and their representatives. This obligation for a preliminary assessment should be read alongside the requirements set forth in Articles 26(9) and 27(4) of the AI Act, concerning data impact assessment and fundamental rights impact assessment, respectively. Together, these provisions aim to enhance the regulatory framework established by the GDPR by establishing a series of obligations and constraints on the information flow from the provider to the deployer of an AI system, to better understand and evaluate the impact of its operation (Peruzzi, 2023). Furthermore, guaranteeing prior consultation with workers and their representatives before drafting the assessment document is of primary importance, as it enables informed interaction that can enhance the effectiveness of the risk assessment.

Subsequently, Article 9 of the Directive introduces extensive information obligations for platforms towards workers, their representatives, and, upon request, the relevant national authorities.

Specifically, for both types of algorithmic systems (monitoring and decision-making), a general obligation exists to provide information on the use or commencement of any experimental phase of these systems (Rosin, 2022).

With particular regard to monitoring systems, platforms must disclose the categories of data and activities subject to monitoring, including client evaluations; the monitoring objective and the methods by which the system aims to achieve it; the recipients or categories of recipients of personal data processed by such systems; and any transmission or transfer of this personal data, even within a group of companies (Article 9, Paragraph 1, b).

In relation to automated decision-making, an obligation exists to provide information on "all types of decisions supported or made by automated systems", even if these decisions do not significantly impact platform workers.

More specifically, platforms are required to disclose the categories of data, the main parameters, and the reasons underlying decisions that affect a worker's contractual status or decisions with adverse effects, particularly regarding non-payment, or the restriction, suspension, or closure of a worker's account (Article 9, Paragraph 1, c).

However, the requirement that the above-mentioned information must be provided "no later than the first working day" is unclear, as it would be preferable to recognize a prior information obligation (at the time of registration on the platform, and therefore even before receiving the first job assignment). Nonetheless, it is commendable that the Directive specifies that workers (Article 9, Paragraph 3) or their representatives may request this information "at any time", and that this right also extends to prospective platform workers when automated tools are used in the hiring process (Article 9, Paragraph 5).

In the Directive, the principle of algorithmic transparency is complemented by two fundamental guarantees: (a) human monitoring of automated systems (Article 10), which must be carried out periodically (at least every

two years) by qualified human personnel to assess specific risks, particularly those related to health and safety, as well as ensuring equal treatment for platform workers; and (b) contestation and human review of automated decisions (Article 11), with an obligation to provide written justification for any decision that limits access to work or its remuneration. However, the requirement for written justification could easily be circumvented by automatic text-generation systems, which allow machines to provide a generic justification independently. Therefore, to ensure the effectiveness of this provision, it seems essential to interpret the guarantee of "written justification" as personalized justification (related to the specific case) drafted by human personnel.

Finally, to seal the framework of protections, on one hand, Article 16 strengthens the investigative powers of the judiciary: "national courts or other competent authorities may order platforms to disclose relevant evidence under their control" (Gaudio, 2024, p. 91); on the other hand, Article 18, Paragraph 2, establishes that the digital labour platform is required to provide justification for any decision to exclude a worker from the system (digital cold dismissal).

The regulation of algorithmic management in terms of algorithmic transparency under this Directive is essential, as it represents the first structured regulation of this phenomenon. However, two necessary issues arise regarding the risks of algorithmic opacity. First, the Directive applies solely to the field of digital platform work, which is indeed one of the most prevalent forms of algorithmic management but by no means the only one. Consequently, outside platform work, the protection of other forms of algorithmic management is left to the independent initiatives of individual member states.

For example, In Italy, Spain, and Germany, rights to algorithmic transparency have been introduced for all employment relationships involving the use of automated decision-making or monitoring systems (Corti, 2023; Cardo, 2022; Doellgast, Wagner, & O'Brady, 2023).

Additionally, a second crucial issue emerges regarding European legislation: The algorithmic transparency safeguards outlined in Directive No. 2831/2024 need to be supplemented by a guarantee of algorithmic comprehensibility or explainability.

Algorithmic Transparency and Explainability Through an Integrated Approach

The effectiveness of algorithmic transparency rights, introduced in European law regarding individual aspects of platform work, depends on the concrete "explainability" of algorithmic functioning.

This algorithmic explainability requires a technical synthesis of relevant information, requested "upstream", which ideally should be carried out not by the employer or client, but by collectively organized entities with prior training (Gaudio, 2024). Otherwise, there is a risk of imposing an "information overload" that would still be ineffective in redressing workers' informational asymmetries (Zappalà, 2023, p. 623).

On this point, Directive No. 2024/2831/EU clarifies in Article 9, Paragraphs 2 and 3, that transparency information must be concise, transparent, intelligible, and easily accessible. However, the reference to "conciseness" appears vague and of limited utility on its own to ensure genuinely informed awareness among workers. Indeed, there is no guarantee that algorithmic transparency rights will automatically translate into a "right to algorithmic understanding". While this right is generally not covered by Directive No. 2024/2831/EU, it has been introduced into the legal framework through Article 86 of the AI Act. Under this article,

> a person affected by a decision based on the output of a high-risk AI system, which produces legal effects or significantly impacts their health, safety, or fundamental rights, has the right to obtain from the deployer (employer or client) clear and meaningful explanations about the role of the AI system in the decision-making process and the main elements of the decision made.

On the topic of algorithmic explainability, although the Platform Work Directive does not contain an express provision equivalent to Article 86 of the AI Act, the algorithmic transparency safeguards provided in Articles 10 and 11 of the Directive—including the obligation of human oversight, the right to explanation, and human review of algorithmic decisions—appear to be aligned with this objective. The requirements for human supervision and monitoring of the algorithm's functioning, combined with the obligation of written justification, may indeed lay the groundwork for establishing an independent right to "algorithmic explainability". In particular, the right to obtain from the platform, without delay, a transparent and intelligible explanation for any decision made or supported by an automated system helps to resolve doubts regarding the existence, within data protection law (specifically Article 22 of the GDPR), of an independent right to an explanation of the impact and functioning of automated processes (Wachter, Mittelstadt, & Floridi, 2017; Malgieri & Comandé, 2017).

In conclusion, transparency protections are essential to mitigate the risks associated with opaque and uncontrollable management practices. An integrated interpretation of the GDPR, the AI Act, and the Platform Work Directive supports the recognition of a new right to algorithmic comprehensibility and/or explainability. However, it is important to emphasize that this integrated reading cannot fully address the limitations stemming from the lack of a comprehensive regulatory framework for algorithmic management.

A more cohesive and less fragmented European regulatory approach would have been desirable, one grounded in the recognition of next-generation (digital) rights aimed at protecting workers' dignity and freedom from arbitrary and abusive practices concealed within algorithmic organization not only on platforms but in digital and algorithmic enterprises more broadly.

Furthermore, for the effectiveness of these safeguards, it is essential that rights to information on the functioning and impact of algorithms are recognised by collective representatives (both self-employed and employees). Collective actors must understand algorithmic operations to better protect individual rights and strengthen collective bargaining, which can also serve as an effective tool for early regulation of automated systems (De Stefano, 2018).

Concluding Remarks

Considering the analysis conducted so far, it can be concluded that although there is no unified regulatory framework (which would certainly be desirable) regarding the algorithmic management of labour relations, the European Union legal system is marked by various legal provisions that can be invoked to mitigate the risks of algorithmic opacity, both preventively and remedially.

Among these, particular emphasis should be placed on data protection safeguards and anti-discrimination protections, which serve as external limits to the employer's organizational and control power (including in its automated form) and as instruments that can be invoked, even by collective actors, to assess the impact of automated systems on fundamental rights in judicial proceedings.

However, it has also been observed that in relation to the "meta-risk" of algorithmic opacity, the effectiveness of the GDPR and anti-discrimination law is weakened by increasing informational asymmetries (Prassl, 2022), which make it extremely difficult for workers to understand the effects produced by the algorithmic system. In the absence of understanding and recognition of the prejudice suffered, invoking existing protections in legal proceedings becomes more challenging.

To strengthen the effectiveness of these protections, it is argued that it is necessary to promote, through a proactive and precautionary approach, specific "algorithmic transparency" rights that should be operational before the introduction or use of automated systems in all labour relations impacted by algorithmic management.

Important protections in this regard have been introduced with respect to platform work by Directive No. 2831/2024; however, its limited scope of application does not provide sufficient protection against the risks of algorithmic management within the European context.

Some more generalized provisions can be found in the AI Act, which has the merit of introducing a right to algorithmic explainability; however, there is a lack of specific provisions on algorithmic transparency tailored to the particularities of labour relations.

Therefore, while an integrated interpretation of anti-discrimination, privacy, and algorithmic transparency rules is helpful, it cannot be assumed that these legal segments will fully resolve the problem of understanding how algorithms operate, especially the more complex ones.

The best solution appears to be the adoption of an independent regulatory framework for algorithmic management in labour relations, which would introduce specific rights to algorithmic transparency, explainability of automated actions, and provide a facilitated burden of proof for workers. Moreover, it seems essential to steer the development of algorithms toward a principle of readability by design and by default (following the path already outlined by the GDPR around privacy).

This approach could make a difference, as the promise of fairness, rationality, and objectivity in the digital revolution is not necessarily destined to remain an illusion.

Algorithmic decisions are potentially more traceable and controllable than human ones, and, in general, technology is the object of action, not the acting subject: It merely provides us with tools, and their impact—whether positive or negative—on the real world depends on the choices that guide their construction, use, and regulation.

References

Aloisi, A. (2024). 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, 40*(1), 37-70.

Aloisi, A., & Gramano, E. (2019). Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context. *Comparative Labor Law & Policy Journal, 95*, 105-108.

Adams, Z., & Wenckebach, J. (2023). Collective regulation of algorithmic management. *European Labour Law Journal, 14*(2), 211-229.

Adams-Prassl, J., Abraha, H., Kelly-Lyth, A., Silberman, M., & Rakshita, S. (2023). Regulating algorithmic management: A blueprint. *European Labour Law Journal, 14*(2), 124-151.

Abraha, H. (2023). Regulating algorithmic employment decisions through data protection law. *European Labour Law Journal, 14*(2), 172-191.

Bednarowicz, B. (2019). Delivering on the European pillar of social rights: The new directive on transparent and predictable working conditions in the European Union. *International Labour Journal, 48*(4), 604-623.

Biasi, M. (2024). Intelligenza artificiale e processo: Verso un robot-giudice per le controversie lavoristiche? In *Diritto del lavoro e intelligenza artificiale* (pp. 737-760). Milano: Giuffré

Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), 1-12.

Broecke, S. (2023). Artificial intelligence and labour market matching. *OECD Social, Employment and Migration Working Papers, No. 284*. Paris: OECD Publishing.

Cardo, I. A. (2022). Decisiones automatizadas y discriminación algorítmica en la relación laboral: ¿hacia un Derecho del Trabajo de dos velocidades? *Revista española de derecho del trabajo*, (253), 135-188.

Carinci, M. T., & Dorssemont, F. (Eds.). (2021). *Platform work in Europe towards harmonisation?* Cambridge: Intersentia.

Cefaliello, A., & Kullmann, M. (2022). Offering false security: How the draft artificial intelligence act undermines fundamental workers' rights. *European Labour Law Journal, 13*(4), 542-562.

Corti, M. (2023). L'intelligenza artificiale nel decreto trasparenza e nella legge tedesca sull'ordinamento azienda. *Federalismi, 29*, 163-170.

Cristofolini, C. (2024). Navigating the impact of AI systems in the workplace: Strengths and loopholes of the EU AI Act from a labour perspective. *Italian Labour Law E-Journal, 17*(1), 75-103.

Dastin, J. (2018). *Amazon scraps secret AI recruiting tool that showed bias against women*. London: Reuters.

De Gregorio, G., & Dunn, P. (2022). The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review, 59*(2), 473-500.

De Petris, P. (2024). La discriminazione algoritmica. Presupposti e rimedi. In M. Biasi (Ed.), *Diritto del lavoro e intelligenza artificiale* (pp. 121-151). Milano: Giuffré

De Stefano, V. (2018). "Negotiating the Algorithm": Automation, artificial intelligence and labour protection. *ILO Employment Working Paper, No. 246.* International Labour Office, Geneva.

De Stefano, V. (2022). The EU Commission's proposal for a directive on platform work: An overview. *Italian Labour Law E-Journal, 15*(1), 1-11.

De Stefano, V., & Wouters, M. (2022). AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework. *Osgoode Legal Studies Research Paper, No. 4144899*. York University.

Doellgast, V., Wagner, I., & O'Brady, S. (2023). Negotiating limits on algorithmic management in digitalised services: Cases from Germany and Norway. *Transfer: European Review of Labour and Research, 29*(1), 105-120.

Durovic, M., & Corno T. (2024). The privacy of emotions: From the GDPR to the AI Act, an overview of emotional AI regulation and the protection of privacy and personal data, privacy. In M. Ebers and K. Sein (Eds.), *Privacy, data protection and data-driven technologies* (pp. 368-404). London: Routledge.

Gaudio, G. (2023). Algorithmic bosses can't lie! How to foster transparency and limit abuses of the new algorithmic managers. *Comparative Labor Law & Policy Journal, 42*, 707-741.

Gaudio, G. (2024). Litigating the algorithmic boss in the EU: A (legally) feasible and (strategically) attractive option for trade unions? *International Journal of Comparative Labour Law and Industrial Relations, 40*(1), 91-110.

Gellert, R. (2020). *The risk-based approach to data protection*. Oxford: Oxford University Press.

Georgiou, D. (2022). The new EU directive on transparent working conditions in the context of new forms of employment. *European Journal of Industrial Relations, 28*(2), 193-210.

Giovannone, M. (2024). Il lavoro tramite piattaforma nell'ordinamento europeo. In M. Biasi (Ed.), *Diritto del lavoro e intelligenza artificiale* (pp. 497-525). Milano: Giuffré

Gramano E. (2021). On the notion of "worker" under EU law: New insights. *European Labour Law Journal, 12*(1), 98-101.

Hammedi, W., Leclercq, T., Poncin, I., & Alkire (Née Nasr), L. (2021). Uncovering the dark side of gamification at work: Impacts on engagement and well-being. *Journal of Business Research, 122*, 256-269.

Ingrao, A. (2022). La protezione dei dati personali dei lavoratori nel diritto vivente al tempo degli algoritmi. In R. Santucci and A. Bellavista (Eds.), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori* (pp. 127-138). Torino: Giappichelli.

Kellogg, K. C., Valentine, M., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals, 14*(1), 366-410.

Kinowska, H., & Sienkiewicz, L. (2023). Influence of algorithmic management practices on workplace well-being—Evidence from European organisations. *Information Technology & People, 36*(8), 21-42.

Krzywdzinski, M., Evers, M., & Gerber, C. (2024). Control and flexibility: The use of wearable devices in capital-and labor-intensive work processes. *ILR Review, 77*(4), 506-534.

Kelly-Lyth, A., & Thomas, A. (2023). Algorithmic management: Assessing the impacts of AI at work. *European Labour Law Journal, 14*(2), 230-252.

Kelly-Lyth, A. (2023). Algorithmic discrimination at work. *European Labour Law Journal, 14*(2), 152-171.

Lane, M., & Saint-Martin, A. (2023). The impact of Artificial Intelligence on the labour market: What do we know so far? *OECD Social, Employment and Migration Working Papers, No. 256*. Paris: OECD Publishing.

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law, 7*(4), 243-265.

Otto, M. (2019). Workforce analytics v fundamental rights protection in the EU in the age of big data. *Comparative Labor Law & Policy Journal, 40*, 389-404.

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

Perulli, A., & Bellomo, S. (2021). *Platform work and work 4.0: New challenges for labour law*. Padova: Cedam.

Peruzzi, M. (2023). *Intelligenza artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela.* Torino: Giappichelli.

Ponce Del Castillo, A. (Ed.). (2024). *Artificial intelligence, labour and society.* Brussels: ETUI Printshops.

Pizzoferrato, A. (2021). Digitalisation of work: New challenges to labour law. *Argomenti di Diritto del Lavoro, 6*, 1329-1369.

Prassl, J. (2018). *Humans as a service: The promise and perils of work in the gig economy.* Oxford: Oxford University Press.

Prassl, J. (2022). Regulating algorithms at work: Lessons for a "European Approach to Artificial Intelligence". *European Labour Law Journal, 13*(1), 30-50.

Prassl, J., Binns, R., & Kelly-Lyth, A. (2022). Directly discriminatory algorithms. *The Modern Law Review, 86*, 144-175.

Rosin, A. (2022). Towards a European employment status: The EU proposal for a directive on improving working conditions in platform work. *Industrial Labour Journal, 51*(2), 478-493.

Santagata De Castro, R. (2021). Anti-discrimination law in the Italian courts: The new frontiers of the topic in the age of algorithms. *WP C.S.D.L.E. "Massimo D'Antona". IT, 440*, 1-32.

Santucci, R. (2024). Intelligenza artificiale e diritto del lavoro: L'incontro nelle piattaforme digitali di lavoro. In R. Santucci and A. Trojsi (Eds.), *Diritto del lavoro e intelligenza artificiale tra rischi e benefici*, forthcoming publication.

Senatori, I. (2020). The European framework agreement on digitalization: A whiter shade or pale? *International Labour Law European Journal, 13*(2), 159-175.

Shalev-Shwartz, S., & Ben-David, S. (2014). *Understanding machine learning: From theory to algorithms.* Cambridge: Cambridge University Press.

Smorto, G., & Donini, A. (2024). L'approvazione della direttiva sul lavoro mediante piattaforme digitali. *Labour & Law Issues, 10*(1), 25-44.

Tosoni, L. (2021). The right to object to automated individual decisions: Resolving the ambiguity of Article 22(1) of the General Data Protection Regulation. *International Data Privacy Law, 11*, 145-162.

Waas, B. (2022). Artificial intelligence and labour law. *HSI-Working Paper No. 17.* Hugo Sinzheimer Institut für Arbeits- und Sozialrecht (HSI), Hans-Böckler-Stiftung, Frankfurt a. M.

Wachter, S., Mittelstadt, B. D., & Floridi, L. (2017). Why a right to explanation of automated decision making does not exist in the general data protection regulation. *International Data Privacy Law, 7*(2), 76-99.

Zappalà, L. (2023). Transparency and comprehensibility of working conditions and automated decisions: Is it possible to open the black box? *Italian Labour Journal, 9*, 623-651.

Zilli, A. (2022). *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela.* Pisa: Pacini Editore.