HUNGARIAN LABOUR LAW
E-JOURNAL

# "United we stand, divided we fall".
## *A study on potential legal measures to fight algorithmic discrimination.*

**Federica Palmirotta**[*]

### Abstract

The adoption of algorithms and Artificial Intelligence within the world of work entails new risks, for instance the harm of algorithmic discrimination for workers.

Currently, labour lawyers are trying to assess the adequacy of the current antidiscrimination law framework to address the challenges that digitalisation and algorithmic management pose, despite also highlighting some of its limitations.

Thus, the aim of this paper is to focus on the other legal sources or legal proposals on the European Union level that address issues linked with algorithmic management and, consequently, algorithmic discrimination, in order to investigate whether and how these legal measures corroborate the non-discrimination law framework.

To this end, focus is placed on the General Data Protection Regulation, the AI act, as well as the Directive on improving working conditions in platform work, with the aim to select the regulations which constitute valuable additions to the non-discrimination and equal treatment law and could be useful to prevent, detect and redress algorithmic discrimination, enforcing equality obligations.

The joint analysis of these regulatory sources shows that each of them, despite its shortcomings, provides some forms of protection against discriminations and, indirectly, addresses some of the limitations acknowledged in the antidiscrimination law, therefore, confirming that the interplay of these provisions, if enforced effectively, could become a potential solution against algorithmic discrimination, while also representing an opportunity to correct biases already happening in humans' mind and yet opaque and not explicit.

[*] Research Fellow, University of Modena and Reggio Emilia.

**Keywords:** algorithmic management; platform work; digitalisation of work; antidiscrimination law; prevention of discrimination

## 1. Introduction

The deployment of algorithms in the employment context to manage the workforce has become progressively common in a wide range of sectors in the conviction that these systems make objective and low-cost organisational and managerial decisions, enhance workforce productivity, while reducing the risks of inaccuracy and ensuring neutrality.[1] However, the academia,[2] the news,[3] and even judicial decisions[4] have widely shown that algorithms are biased and perpetuate or exacerbate discriminations.

In the attempt to tackle the significant discriminatory risks inherent of the shift of managerial prerogatives to software machines, labour lawyers are trying to assess the adequacy of the current antidiscrimination law framework to address the challenges that digitalisation and algorithmic management systems ('AMSs') pose.[5] As a matter of fact, the structure of antidiscrimination law is a *sui generis* structure, characterized by the presence of manifold institutions favourable to the victims. Nevertheless, in some circumstances, its shortcomings have already been underlined, to name a few: the high frequency of indirect and collective discriminations, which, given the well-known 'opacity' of algorithms, leads to a strive in the identification of hidden discriminatory practices and, as a consequence, in the collection of evidence;[6] the possibility for a justification to avoid the application of antidiscrimination prohibition;[7] the reliance on causation rather than correlation, which is, instead, one of the techniques adopted by algorithms to process data.

[1] Marta Otto: Workforce Analytics v Fundamental Rights Protection in the EU in the Age of Big Data. *Comparative Labour Law & Policy Journal,* vol. 40. (2019) 392.

[2] See in academia: Ben Wagner et al.: *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications.* DGI (2017), Prepared by the Committee of Experts on Internet Intermediaries (MSI-NET) for the Council of Europe, 2018.; Janneke Gerards – Raphaele Xenidis: *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law.* Luxembourg, Publications Office of the European Union, 2021.; Pauline T. Kim: Data-Driven Discrimination at Work. *William & Mary Law Review,* vol. 58, issue 3. (2017) 857.; Jon Kleinberg – Jens Ludwig – Sendhil Mullainathan – Cass R. Sunstein: Discrimination in the Age of Algorithms. *Journal of Legal Analysis,* vol. 10. (2018) 113–174.

[3] See in the news: Cathy O'Neil: How algorithms rule our working lives. *The Guardian,* 1 September 2016., available at: https://tinyurl.com/3fcyum3c (last accessed 24 March 2023).; Hanna Devlin: AI programs exhibit racial and gender biases, research reveals. *The Guardian,* 13 April 2017, available at: https://tinyurl.com/9pd38maws (last accessed 24 March 2023).

[4] With regards to the judicial decisions, the reference is to the ruling against Deliveroo from the Tribunal of Bologna, 31 December 2020.

[5] Antonio Aloisi: Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights. *Italian Journal of Comparative Labour Law and Industrial Relations,* vol. 40, issue 1. (2024) 37–70.; Gisella De Simone: Discriminazione. In: Marco Novella – Patrizia Tullini (eds.): *Lavoro digitale.* Turin, Giappichelli, 2022. 127–152.; Giovanni Gaudio: 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,* vol. 40., issue 1. (2024) 91–130.; Venera Protopapa: *Uso strategico del diritto e azione sindacale.* Bologne, Il Mulino, 2022.; Marco Peruzzi: Il diritto antidiscriminatorio al test di intelligenza artificiale. *Labour and Law Issues,* vol. 7 (2021).

[6] Frederik J. Zuiderveen Borgesius: Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The Internaional Journal of Human Rights,* vol. 24., no. 10. (2020) 1577.

[7] Ibid. 6.

The present contribution fits into this entangled scenario, with the aim to address the following research question: whether and to what extent existing or proposed regulatory instruments could be effective – at least potentially – to meet the concern raised by AMSs that the Antidiscrimination *acquis* fails to handle and with the desirable result of corroborating the antidiscrimination law framework and improving the conditions of workers in the context of digitised work.

To this end, the study will focus on three legal measures, which should be considered of utmost importance with regards to AMSs deployed in the employment context: namely, the General Data Protection Regulation (henceforth 'GDPR', Regulation EU 2016/679), as well as the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence[8] (henceforth, 'AI Act') and the European Commission Proposal for a Directive on improving working conditions in platform work (henceforth, 'PWD')[9]. The latter are both legal initiatives proposed by the EU Commission to contribute to the building of trustworthy AI and to improve working conditions for digital workers, whose legislative procedure is coming to an end thanks to the positive endorsement of the EU institutions.

The joint analysis on these three legal instruments is supposed to make some progress in this research field, which, up until now, has limited its area of investigation on both non-discrimination law and data protection law[10] and, more recently, both these regulatory measures together with the PWD,[11] when dealing with legal instruments for defending people against discrimination.

The contribution aims at creating a guidance to tackle algorithmic discrimination on an interdisciplinary basis by the examination of these legal instruments through a selection of the provisions which constitute valuable additions to the antidiscrimination and equal treatment law and could be useful to prevent, detect and redress algorithmic discrimination, while enforcing equality obligations.

The paper is structured as follows. After this introductory section, Section 2 opens with a preamble on AMSs and their discriminatory impact, with a view to point out the shortcomings of the antidiscrimination law framework in tackling algorithmic discrimination. Section 3 is devoted to the GDPR, in the pursuit of highlighting the merit and pitfalls of this Regulation with regards to the unveiling of discriminatory practices hidden in AMSs, in particular, investigating how its provisions could have a preventive effect against discriminations. Section 4 deals with the advantages

[8] COM (2021) 206 final, 21 April 2021.

[9] COM (2021) 762 final, 9 December 2021.

[10] See, for instance, W. Schreurs et al.: Cogitas, ergo sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. In: Mirelle Hildebrandt – Serge Gutwirth (eds): *Profiling the European Citizen. Cross-Disciplinary Perspectives.* The Nether Springer, 2008.; R. Gellert – K. De Vries – P. De Hert – S. Gutwirth: A Comparative Analysis of Anti-discrimination and Data Protection Legislations. In: Bart Custers et al. (eds.): *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases.* Dordrecht, Springer, 2013. 61–89.; Borgesius (2020) op. cit.; Aloisi (2024) op. cit.

[11] Giovanni Gaudio: L'algorithmic management e il problema della opacità algoritmica nel diritto oggi vigente e nella Proposta di Direttiva sul miglioramento delle condizioni dei lavoratori tramite piattaforma. *Lavoro Diritti Europa,* vol. 1. (2022) (hereinafter: Gaudio (2022a)].

and the limitations of the AI Act, highlighting its efforts in building better AI systems from the get-go. Section 5 focuses on the PWD and, notably, on the step forward that this Directive could make with the interplay of the GDPR. Lastly, section 6 draws a conclusion to this preliminary analysis.

## 2. Tackling Discriminations in Algorithmic Management Systems: the limitations of non-discrimination law

AMSs are automated or semi-automated computer processes which deal with one of the following activities: (1) workforce planning and task allocation; (2) dynamic piece rate pay setting per task; (3) controlling workers by monitoring, steering, surveiling or rating their work and the time they need to perform specific tasks, nudging their behaviour; (4) measuring actual worker performance against predicted time and/or effort required to complete task and providing recommendations on how to improve worker performance and (5) penalising workers, for example, through termination or suspension of their accounts.[12] To sum up, in AMSs all the operations which once were prerogatives of the employers, are being performed by computer machines.

The first application of this management system lays in the gig-economy, with platforms using algorithmic systems and ratings to allocate tasks and manage the workforce. Since then, the platform-based work has long constituted a laboratory for the development of algorithmic management devices, which are now entrenched in workplaces of any economic sector.[13]

Notwithstanding the manifold advantages that AMSs grant employers in terms of increase in the workforce productivity as well as faster and objective managerial decisions, these systems entail discriminatory risks, which, according to the literature,[14] may be caused by either managerial choices, facilitated by the ‘opacity’ of algorithms, or structural characteristics which compromise the algorithm.

The former circumstance involves an intentional discrimination,[15] since the employers uses consciously data mining to hide a discriminatory impact on a protected group. The algorithm, thus, becomes the pretext or justification for differential treatment, which however remains difficult to identify due to lack of transparency.

On the contrary, structural *bias* depend on: the prejudices that the programmer of the algorithm is likely to perpetuate in the algorithm itself; the quality and reliability of the data with which the algorithm is fed; and, finally, the correlations that the algorithm identifies between the data processed and that can be closely linked to the protected grounds of discrimination. This last circumstance is

[12] Aida Ponce Del Castillo – Diego Naranjo: Regulating algorithmic management. *ETUI Policy Brief-European Economic, Employment and Social Policy,* August, 2022.

[13] Jeremias Adams-Prassl: What if your Boss was an Algorithm? Economic Incentives, Legal Challenges and the Rise of Artificial Intelligence at Work. *Comparative Labour Law & Policy Journal,* vol. 41. (2019) 131.

[14] Gerards–Xenidis (2021) op. cit.; Kim (2017) op. cit.; Kleinberg–Ludwik–Mullainthan–Sunstein (2018) op. cit.

[15] Kim (2017) op. cit. 884.

peculiar and derives from the ability of the algorithms to group the data in clusters, on the basis of variables apparently neutral, but in fact connected to the grounds of discrimination. Variables with these characteristics are defined in literature as 'proxy'.[16] One example is the use of the postal code, often related to ethnic origin.

In order to challenge the existence of discriminatory practises, victims or their representative may bring legal actions to Courts, benefiting from the non-discrimination law, resulting from the EU Directives, and its 'legal opportunity structure',[17] whose characteristics are built in favour of the victims, in consideration of the unbalanced relationship that each discrimination implies. However, the non-discrimination law may present some limitations with regards to discriminations occurring in digital context mediated by algorithms.

Firstly, in the antidiscrimination law there is a strong emphasis on causation linked to the protected grounds in order to detect discrimination, which isn't tailored to suit the peculiar functioning of data processing in AMSs that, instead, as it has already been stated, is more rather based on correlation and on the identification of classes assembled with characteristics not manifestly considered protected grounds or associated with such grounds.[18] In the absence of evidences – even statistical ones – confirming the causation linked with such protected grounds, this system may leave unprotected some victims of discrimination. Besides, even when the causation is confirmed, the mechanism of AMSs leads to an increased frequency of indirect discrimination, for which the antidiscrimination law provides more scope for justification.[19] Indeed, in cases of indirect discriminations, the prohibition of discrimination doesn't apply if the alleged discriminator invokes an objective discrimination, meeting the proportionality and necessity requirements.[20]

Secondly, algorithmic profiling is based on a huge quantity of personal and behavioural data which heightens the risks for intersectional discriminations, a concept that has long remained undefined at EU level.[21]

[16] Raphaele Xenidis – Linda Senden: EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination. In: Ulf Bernitz – Xavier Groussot – Jaan Paju – Sybe A. De Vries (eds.): *General Principles of EU Law and the EU Digital Order*. Kluwer Law International, 2020.

[17] This notion, developed in legal mobilisation studies, refers to the degree of openness – or "liberality" – of the legal system to strategic action, taking into account the procedural elements (for example, the rules on standing or burden of proof) and the substantive elements (including, the presence of enforceable rights and/or precedents in favour), which jointly influence the choice of actors to undertake judicial strategies and condition the possibility of obtaining a favourable decision. See Protopapa (2022) op. cit. 33.

[18] Aloisi (2024) op. cit.; Adams-Prassl (2019) op. cit., 123. The issue of justification is also highlighted by Sylvaine Laulom: Discriminations by Algorithms at Work. In: Tamás Gyulavári – Emanuele Menegatti (eds): *Decent work in the digital age: European and comparative perspectives.* Oxford, Hart Publishing, 2022. 271–290., although she adopts a favourable view with regards to the adequacy of the antidiscrimination framework to tackle algorithmic discriminations.

[19] Adams-Prassl (2019) op. cit. 41.; Borgesius (2020) op. cit. 1577.

[20] Article 2, par. 2, (b), Directive 2000/78/CE.

[21] It must be noted that this concept has been finally recognised by law. Its regulation has been attempted by the Directive EU 2023/970, which at Article 3, par. 2, (e) defines it as "discrimination based on a combination of sex and any other ground or grounds of discrimination protected under Directive 2000/43/EC or 2000/78/EC" and invites Member States to consider the increased damage deriving from this phenomenon, justifying higher compensation. See also Recitals 25, 32 and Articles 16, 23, 29, Directive EU 2023/970 in this regard.

Another significant limitation of the non-discrimination law comes from the 'opacity' of algorithms. According to scholars, the opacity can be linked to three different reasons: (1) intentional corporate concealment; (2) technical illiteracy, which means that sometimes having access to the code will not be sufficient to fill the gap; (3) inherent characteristics of machine learning systems, whose machine optimizations based on training data do not naturally accord with human semantic explanations.[22]

This opacity reduces the awareness of the victims[23] and hinders the collection of evidence to prove the discrimination. As a matter of fact, even if the legal system requires a lighter burden of proof for the victims, they still have to establish facts from which it may be presumed that there has been direct or indirect discrimination,[24] as well as a comparation with a non-discriminated subject, however, most of the time they lack the necessary information and they have trouble in the identification of the actual discriminator.

Furthermore, the antidiscrimination *acquis* has been conceived mostly as a structure to counteract and remove discriminations already happening, which, hence, usually requires the activity of the victims in taking legal action before the Courts, leaving little space for prevention, not to mention the fact that victims does not always take legal action either due to economic and cultural issues or because they want to avoid direct exposure in court, fearing retaliatory behaviour by the employer.

In the next sections, it will be described how these limitations may find support in other regulatory instruments.

## 3. GDPR addressing data-driven discriminations: from prevention to enforcement

In countries where scholars have begun to focus on the interaction between data protection and discrimination, there is a clear consensus on the importance of the GDPR in the fight against algorithmic discrimination.[25]

Indeed, as it will be demonstrated *infra*, the GDPR provides a set of complex measures that can be considered an upstream form of protection against discrimination, while the non-discrimination law could be located rather downstream, performing its best as an instrument of strategic litigation.

As regards the application of the GDPR in this field, it should appear indisputable, considered that AMSs process personal data of employees and unemployed persons in order to analyse and forecast aspects of their work performance, but also potentially their health, reliability, behaviour, location and movements. These operations fall under the notion of 'profiling', according to the interpretation of the

[22] Jenna Burrell: How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society,* vol. 3., Iss. 1. (2016).

[23] Borgesius (2020) op. cit. 1577.

[24] Article 10, Directive 2000/78/CE.

[25] Birte Book – Susanne Burri – Linda Senden – Alexandra Timmer: *A comparative analysis of gender equality law in Europe 2021.* Luxembourg, Publication Office of the European Union, 2022. 95.

GDPR , which involves “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.[26] Therefore, employers adopting AMSs should meet the legal requirements defined in the GDPR.[27]

From an early analysis of the provisions in the GDPR, it is evident that this regulation is intended to foster transparency in data processing – and thus, in AMSs – also with regards to discriminatory effects that may result from processing of sensitive personal data. By contrast, it is curious to note that the notion of ‘discrimination’ appears in the GDPR only three times.[28]

However, an almost evident correlation with non-discrimination law and data protection regulation may be found in Article 9, which identifies ‘special categories of personal data’ or ‘sensitive data’, for which the law provides specific protection considered that their processing might create significant risks to fundamental rights and freedoms. In this regard, the GDPR qualifies as ‘sensitive’ data related with: race or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health, genetic and biometric characteristics, as well as sex life or sexual orientation.[29] This list of categories overlaps to some extent the list of grounds of discrimination protected under EU non-discrimination law. Nevertheless, some important grounds, in whose regard the antidiscrimination *acquis* is particularly developed, are set aside, namely: gender, disability and age. Although disability might be included in the term ‘health’, still age and gender remain difficult to read in these provisions and are considered common personal data, under the GDPR.[30] Despite this and regardless of the special protection granted to sensitive data, the GDPR aims at regulating and safeguarding processing of personal data of any kind, as long as it is an information relating to an identified or identifiable person,[31] and, to this end, this Regulation prevents – at least in theory – discrimination based on each protected ground of discrimination.

Moving forward to the investigation of the GDPR’s rules devoted directly or indirectly to the fight against discrimination, it is possible to select manifold provisions that deal notably with the prevention and avoidance of discriminations from the get-go, as well as provisions that concerns the enforcement and the remedies provided in case of violation of GDPR’s requirements, which indirectly strengthen the enforcement of non-discrimination law as well.[32]

[26] Article 4, (4) GDPR.

[27] Otto (2019) op. cit. 396.

[28] Recital 71, 75, 85, GDPR.

[29] Article 9, par. 1, GDPR.

[30] Gerards–Xenidis (2021) op. cit. 49.

[31] Article 4, (1), GDPR.

[32] This distinction is suggested by the author in consideration with the specific purpose of the present contribution.

The first group of provisions includes undoubtedly the principles relating to processing of personal data stated in Article 5,[33] especially the principle of lawfulness, fairness, transparency and accuracy. The compliance with these principles in itself would be able to hinder the existence of disparate treatments, and, most importantly, it would hamper two of the characteristics of AMSs entailing discriminatory risks as identified *supra*: the opacity and the structural *biases* due to inaccuracy in the dataset. Moreover, the 2nd paragraph of Article 5 regulates the principles of accountability, together with Article 24, requiring the controller – in this context, employer – to demonstrate compliance with these principles. Among commentators, there is a general consensus that these provisions actually reverse the burden of proof.[34] As it is well-known, the shift of the burden of proof is particularly significant in circumstances with imbalance of powers between the parties and, especially, in the context of algorithmic 'black-box', since it requires the employer to disclose relevant information if he doesn't want to yield.[35]

The implementation of the principle of fairness and transparency is referred to in articles 12 to 15, to be analysed jointly with recitals 58 to 62. In particular, article 13 and 14 regulates the right to be informed and require controllers (or employers) to provide data subjects (or employee), at the time when personal data are obtained, with concise and easily accessible information including but not limited to: the purpose of processing; the rights granted (i.e. right to access; right to rectification and erasure; right to lodge a complaint with a supervisory authority); as well as the existence of automated decision-making, including profiling. In this latter circumstance and, precisely, when the decision is based solely on automated processing that produces legal or similarly significant effect[36] the controller must also provide information about the logic involved and explain 'significance and envisaged consequences of the processing'[37]. This means that the controller should inform in an understandable way the data subject firstly about the rationale behind and the criteria relied on in reaching the decision, as well as about intended or future processing and the ways in which the automated decision-making affect the data subject.[38] In spite of this, anytime the processing involves profiling-based decision making, the controller must inform data subjects that the processing is aimed at profiling and that it is supposed to make a decision based on the profile generated.[39]

[33] Article 5, GDPR, identifies the following principles that any processing should follow: (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimisation; (d) accuracy; (e) storage limitation; (f) integrity and confidentiality and (g) accountability.

[34] Paul Voigt – Axel Von Dem Bussche: *The EU General Data Protection Regulation (GDPR). A Practical Guide.* Springer, 2017. 31–32.; Christopher Docksey: Comment to Article 24. In: Christopher Kuner – Lee A Bygrave – Christofer Docksey – Laura Drechsler (eds.): *The EU General Data Protection Regulation (GDPR): A Commentary.* Oxford, Oxford University Press, 2020. 555., who says that the burden of proof shifts to the controller, but only when the data subject has offered *prima facie* evidence of an unlawful processing activity.

[35] Gaudio (2024) op. cit. 12.

[36] See infra about Article 22, GDPR.

[37] Article 13, par. 2 (f) and Article 14, par. 2, (g), GDPR.

[38] Guidelines on Automated individual decision-making and Profiling for the purposes of the Regulation 2016/679 (WP251). 3 October 2017. 25–26. (Hereinafter: WP251)

[39] Ibid. 38.

The right to be informed is also strengthened by the right to obtain access to all the information[40] that should have been provided under Article 13, a right that has been particularly convenient in two legal proceedings to open the algorithmic 'black-box'[41] in order to prove the employee status of workers.

The first case concerns the right of access exercised by a Glovo rider under Article 15, prior to taking legal action before the Tribunal of Palermo,[42] to collect information regarding his working sessions and to prove that the disconnection of his account was due to by his data processing. The latter request wasn't fulfilled by the company, but the rider, potentially, could have filed a complaint with a supervisory authority, thus obtaining even more evidence to be re-classified as an employee.[43]

This happened in the second case,[44] taken before the Amsterdam District Court by Uber and Ola drivers claiming their right to access their personal data as well as information regarding the functioning of the algorithmic management adopted by the companies. In this case, the Court ordered to disclose information about the decisions made, the data analysed and the assumptions justifying the final choice, which allowed platform workers to verify the correctness and lawfulness of the data processing.

In short, these transparency requirements may be fruitful for several reasons.[45] Firstly, as showed in the case discussed in the Tribunal of Palermo, they might be useful to disassemble the opaque decision of the AMSs and to support the allegations to report a discriminatory treatment. Secondly, they also fulfil a preventive function, since they discourage reasonable employers to adopt algorithmic devices that can be made transparent and whose functioning is not biased or discriminatory, given that they will always be required to disclose information.[46] Lastly, they increase the victim's perception of being discriminated, whose lack of awareness, on the opposite, is an obstacle for the enforcement of non-discrimination rights.

The preventive function is also carried out by two other provisions that more directly concern AMSs and discriminatory risks: namely, Articles 9 and 22. With regards to Article 9, as it has been stated *supra*, it provides a specific protection for sensitive data and prohibits its processing from the very beginning, unless one of the exceptions of par. 2 applies. Some scholars criticize this approach, arguing that simply removing certain variables from a model does not ensure predictions that are,

[40] Article 15, GDPR.

[41] Frank Pasquale: *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, Harvard University Press, 2015.

[42] Trib. Palermo 20 November 2022, in which the judge has recognised the employee status of the rider.

[43] Gaudio (2022a) op. cit. 7.

[44] Amsterdam District Court 11 March 2021, C/13/687315/HARK20-207, C/13/689705/HARK/20-258, e C/13/692003/HARK20-302.

[45] Accordingly, Otto (2019) op. cit.; Gaudio (2022a) op. cit.; Gaudio (2024) op. cit.; Aloisi (2024) op. cit.

[46] Giovanni Gaudio: Algorithmic Bosses Can't Lie! How to Foster Transparency and Limit Abuses of the New Algorithmic Managers. *Comparative Labor Law & Policy Journal,* vol. 42. (2022) 707–741. [hereinafter: Gaudio (2022b)].

in effect, uncorrelated to those variables.[47] Indeed, in consideration of discriminatory risks, this approach might be suitable to prevent direct discriminations, but would leave apart indirect ones. Nevertheless, in this regard, the Article 29 Working Party expressly stated that these provisions should be applied even in circumstances in which special categories of data are derived or inferred from profiling activity.[48] This is the case of correlations, that, as it has been already explained, are frequently operated in AMSs. In those circumstances, the controller should make sure that: (1) the processing is not incompatible with the original purpose; (2) they have identified a lawful basis for the processing of the special category data; and (3) they inform the data subject about the processing.

As to the content of Article 22, it is considered to be one of the most promising aspects of GDPR.[49] Indeed, this provision provides a general prohibition on fully automated individual decision-making, included profiling, which produces legal effects or significantly affects data subjects, unless one of the exceptions provided in Article 22, par. 2, applies, namely: contractual necessity; authorisation by Union or MS law; and explicit consent. Firstly, with regards to the impact of decisions to be covered by Article 22, according to the Article 29 Working Party, a legal effect may derive from a processing that impacts either someone's legal rights (such as the freedom of association) or a person's legal status or their rights under a contract (such as: termination of an employment contract); instead, a similarly significant effect materializes when, even if there is no change in their legal rights or obligations, the data subject could still be impacted sufficiently to require the protections under this provision (such as: decisions that deny someone an employment opportunity or put them at a serious disadvantage).[50] In the event in which one of the exceptions applies, there must be measures in place to safeguard the data subject's rights and freedoms and legitimate interests, providing at least the right to obtain human intervention on the part of the controller, which should not be limited to a token gesture, instead it must ensure a meaningful oversight carried out by someone with the authority and competence to change the decision.[51] Moreover, it should be recognised to the data subject the right to express his or her point of view and to contest the decision.

Among the exceptions, the occurrence attributable to labour law and AMSs is the contractual necessity, considered that it is undisputed that in the employment context the consent shouldn't almost unlikely be considered a lawful basis for processing.[52] Still, as provided by par. 4, the exceptions can't be implemented when the decision is based on sensitive data, unless there are both the explicit

[47] Moritz Hardt: How Big Data Is Unfair: Understanding Sources of Unfairness in Data Driven Decision Making. *Medium,* Sep. 26, 2014. https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de ; Matthias Leese: The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-Discriminatory Safeguards in the European Union. *Security Dialogue*, vol. 45., issue 5. (2014) 494–511. https://doi.org/10.1177/0967010614544204

[48] WP251 op. cit. 15.

[49] Michael Veale – Lilian Edwards: Clarity, surprises, and further questions in the Article 29 WP draft guidance on automated decision-making and profiling. *Computer Law Security Review,* vol. 34 (2018) 398–404.

[50] See WP251: op. cit. 21.

[51] Ibid.

[52] See WP259: Guidelines on consent under Regulation 2016/679, 28 November 2017, Revised and Adopted on 10 April 2018.

consent of the data subject or a substantial public interest and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. This implies that AMSs deployed in the employment context, based on solely automated decision making, should never be supposed to take decisions based on sensitive data according to the GDPR. This last observation highlights the different approach of GDPR and non-discrimination law, while the latter is based on the effect/impact of a treatment based on a ground of discrimination, the former – in theory – forbids from the very beginning processing of these special categories of data, regardless of its discriminatory impact, at least in solely automated decision-making systems.

In accordance with the majority of scholars,[53] the last relevant provision to be included in the prevention measures capable to protect people against algorithmic discrimination is the requirement to carry out a Data Protection Impact Assessment (henceforth, DPIA), pursuant to Article 35, whenever a processing is likely to result in a high risk to the rights and freedoms of natural persons. The mandatory requirement of carrying out a DPIA seems unquestionable for employers adopting AMSs, taking into consideration Article 35, par. 3, (a),[54] together with Recital 75, the explanation of the Article 29 Working Party,[55] as well as the relevant narrative in academia.[56]

Concerning the subject of the DPIA, it is intended to be a process to assess, identify and minimise data protection risks. Indeed, it requires controller to adequately prove in which manner and through what instruments they ensure compliance. Moreover, it should be frequently reviewed and regularly re-assessed,[57] fitting into the relentlessly evolving context resulted by the digitalisation of workplace. At the same time, the DPIA should ensure algorithmic legibility and accountability due to allocating a set of duties to the data controller, thus, addressing two significant challenges posed by AMSs, the opacity and the difficulty in finding a responsible, while also establishing the substance for future remedial mechanisms. [58] The preventive function is ensured by the fact that any DPIA should be carried out prior to the processing, shifting once again the focus from *ex post* reparation to *ex ante* rules aimed at inhibiting unfair data processing.[59]

[53] Bryce W. Goodman: A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection. *29th Conference on Neural Information Processing Systems (NIPS 2016).* Barcelona, 2016. https://tinyurl.com/3nkjfwe2; Paul Hacker: Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law. *Common Market Law Review,* vol. 55., no. 4. (2018) 1143–1185.; Margot E. Kaminski – Gianclaudio Malgieri: Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations. *University of Colorado Law Legal Studies Research Paper No. 19–28*, September 18, 2019. https://doi.org/10.2139/ssrn.3456224

[54] Article 35, par. 3, GDPR: "A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. […]"

[55] WP248: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 April 2017.

[56] See, for instance, Otto (2019) op. cit.; Borgesius (2020) op. cit.; Aloisi (2024) op. cit.

[57] WP248 op. cit. 14.

[58] Aloisi (2024) op. cit. 22.

[59] Hacker (2018) op. cit. 1147.

This provision, together with the voluntary certifications pursuant to Article 42, attempts to create an environment devoid of toxic automated systems in the future.[60]

The second group of provisions concerning enforcement and remedies includes Chapter VI (Article 51-60), devoted to the regulation of Supervisory Authority and their powers, as well as Chapter VIII (Articles 79-84), entitled 'Remedies, liability and penalties'.

As a matter of fact, the existence of competent authority with the duty to monitor the compliance with the GDPR, also thanks to relevant *ex officio* investigation powers that do not require a proactivity of the victims of infringements, is more effective to contrast reluctance of companies to share information on the functioning of AMSs, not to mention the greater incisiveness of fines that these Authorities can impose, amounting up to 20 millions EUR or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year. Furthermore, their duty to cooperate with each other across MS at this scope is also particularly favourable in an economic context characterized by dynamic and global relations.

Examples of the effective operation of a Supervisory Authority are the *ex officio* investigations carried out by the Italian Data Protection Authority (Garante per la protezione dei dati personali), in one case also with the cooperation of the Spanish Data Protection Authority (Agencia Española de Protección de Datos), against Foodihno/Glovo[61] and Deliveroo,[62] which were found to infringe several GDPR's requirements and to put in practise discriminatory decision-making and, for this reason, were ordered to comply with the GDPR and pay considerable fines.[63]

In the end, the enforcement infrastructure of the GDPR, while it is intended to require compliance with the data protection requirements, leads indirectly to a greater enforcement of non-discrimination law and, especially, in respect of prohibition of non-discrimination.

After this investigation of GDPR in search of regulatory instruments suitable to fill the gaps of non-discrimination law, it is possible to state that the omnibus data protection architecture in the EU, at least in theory, seems to be vigorous enough to tackle the algorithmic discriminatory challenges posed by AMSs, overcoming some of the limitations of the antidiscrimination framework. Yet, some shortcomings endure. As a matter of fact, the GDPR has an individual approach and does not contemplate remedies for groups,[64] nor it is especially dedicated to employment context, therefore, it does not encompass collective aspects inherent in labour law, including those related to the role of workers' representatives,[65] information and consultation of workers and the role of labour inspectorates

[60] Lilian Edwards – Michael Veale: Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review,* vol. 16. (2017) 77.

[61] Order n. 234, 10 June 2021, Garante per la protezione dei Dati Personali.

[62] Order n. 285, 22 July 2021, Garante per la protezione dei Dati Personali.

[63] The Garante per la Protezione dei Dati Personali issued Foodinho with a € 2.600.000 fine and Deliveroo with a € 2.500.000 fine.

[64] Edwards–Veale (2017) op. cit.

[65] Apart from a space that could be carved out for workers' representative in giving their views with regards to the DPIA, pursuant to Article 35, par. 9, GDPR.

in enforcing labour rights.[66] Furthermore, it should be added that there is a compliance and enforcement deficit, due to both a lack of reliability of several organisations and the overburden of Data protection Authorities, as well as because sometimes the transparency requirements on which is based a large part of this regulation could be impracticable to fulfil given the difficulty or impossibility to explain the logic behind a decision, when an algorithmic system arrives at that decision after analysing large amounts of data and, especially, in machine-learning algorithms,[67] not to mention the absence of a uniform European procedural framework requiring Supervisory Authorities to decide cross-border disputes within strict deadlines.[68]

## 4. AI Act addressing algorithmic discriminations through a risk-based approach

In the attempt to foster excellence and innovation, while building human-centric and trustworthy technologies, the EU Commission has presented a Proposal for a Regulation on Artificial Intelligence, which has been formally approved by the EU Institutions and, once into force after publication in the EU's Official Journal,[69] will complete the patchy legal framework regarding AMSs.

Following a risk-based approach, already adopted by the EU lawmakers with DPIA in the GDPR, the Regulation lays down a uniform, horizontal legal framework for AI that aims to ensure legal certainty and, most notably, to build better AI systems *ab initio*.[70]

To this end, firstly, it identifies the notion of 'AI systems'[71], which undoubtedly includes AMSs; in addition to this, seeking to address the accountability issue, it clarifies which are the subjects liable under the scope of the regulation, distinguishing between 'providers' and 'deployers'. The former are the natural or legal persons, public authority, agency or other body that develop an AI system or that has an AI system developed and places that system in the market under its own name or trademark,[72] while the latter are the natural or legal persons under whose authority the AI system is used, unless such system is used during a personal non-professional activity.[73] Most of the legal obligations provided in this Regulation are allocated to providers, nonetheless, in the employment

[66] These limitations are also underlined in the Explanatory Memorandum combined with the PWD. In this sense, also Antonio Aloisi – Nastazja Potocka-Sionek: De-gigging the labour market? An analysis of the 'algorithmic management' provisions in the proposed Platform Work Directive. *Italian Labour Law e-Journal,* vol. 15., issue 1. (2022) 29–50.

[67] Borgesius (2020) op. cit. 1581.

[68] Ponce del Castillo–Narnajo (2022) op. cit.

[69] The Council has given the final green light to the Regulation on the 21st May 2024. Given that at the time of writing, the legislative act has not yet been published in the EU's Official Journal, the analysis carried out in the present contribution is based on the last version of the text approved, available at: https://tinyurl.com/3ja4b8j6

[70] As it is also suggested by Edwards–Veale (2017) op. cit. 6.

[71] Article 3, (1), AI Act: "machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".

[72] Article 3, (3), AI Act.

[73] Article 3, (4), AI Act.

context, it could be more likely that employers fall under the definition of deployers. This may result in some troubles in the relationship with the employees, since employers may relieve themselves from responsibility.[74]

Stepping forward to the specific content of the AI act, it categorizes AI systems depending on their riskiness and distinguishes between: i) prohibited AI practices (Chapter 2, Article 5); ii) high-risk AI systems (Chapter III); iii) general purpose AI systems (Chapter V). According to the AI act, the second group of provisions applies explicitly to AI systems used in the employment context or in the access to self-employment for recruitment or selection of persons and for making decisions affecting terms of work-related relationships, such as on promotion, termination, task allocation, monitoring or evaluation of persons.[75]

However, regardless of the specific requirements for high-risk AI systems, Article 5 of the endorsed regulation identifies a list of AI practices which are prohibited in advance since they may entail an unacceptable risk. This catalogue includes some practices that can be performed by AMSs, such as the evaluation or classification of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, when the social score leads either to a detrimental or unfavourable treatment of a certain groups in social contexts unrelated to contexts in which data was originally collected or, most notably, to a detrimental or unfavourable treatment of a certain groups which is unjustified or disproportionate to their social behaviour or its gravity.[76] This prohibition is explained by the risks on violation of the right to dignity and non-discrimination, as well as of the values of equality and justice, that such practice entails.[77] There are also other practices, which may be performed by AMSs, prohibited by the new regulation: the risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics (unless it is carried out to assess the involvement of a person in a criminal activity based on objective and verifiable facts); the use of AI systems to infer emotions of a natural person in the areas of workplace (unless for medical of safety reason); the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.

Hence, the AI act adopts an upstream approach, likewise the one adopted by the GDPR, especially in Articles 9 and 22 (4). However, in this circumstance, the subject of the prohibition is not a predefined

[74] Valerio De Stefano – Mathias Wouters: *AI and digital tools in workplace management and evaluation. An assessment of the EU's legal framework*. STOA: Panel for the Future of Science and Technology, Brussels, European Union, 2022. 55.; Edwards Veale – Zuiderveen Borgesius: Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International,* vol. 4. (2021) 104.

[75] Recital 57 and Annex III, no. (4), AI Act.

[76] It should be noted that the first Draft of the AI act limited the prohibition of this practise only to AI systems deployed by public authorities. The final version approved by the Council extends this prohibition to private actors as well.

[77] See Recital 31, AI Act.

sensitive information whose processing is likely to entail discrimination, instead, it is an operation subject to result in a direct or indirect discrimination in itself. Even though no interpretation in the academia or by practitioners, up to know, is made with regards to the notion of 'social behaviour' and 'known or predicted personal or personality characteristics' provided in the AI act, the opinion that these notions include or are even broader than grounds of discriminations can be shared.

As regard high-risk systems, the AI Act sets out a considerable list of mandatory requirements for providers from the need to establish a risk management and data governance system, the obligation to collect documentation and record-keeping, to the need to ensure transparency, human oversight, robustness, accuracy and cyber-security. Considered together all these requirements may prove to be particularly fruitful in preventing algorithmic discriminations in the building of AMSs from the very beginning. An example is provided by Article 10, which concerns the quality of dataset and is aimed at minimising or avoiding structural *biases* that compromise the output of the decision-making system and perpetuate discriminations. To this end, the providers must ensure, for instance, that the dataset has the appropriate statistical properties. The documentation and record-keeping obligations, as well, are convenient measures to collect evidence against discriminations, similarly to what happens with the right to access and the right to be informed within the GDPR. As a matter of fact, under Article 77, par. 1, the AI Act provides national public authorities and bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights, including the right to non-discrimination, with an investigation power, allowing them to request and access any documentation created or maintained under the AI Act.

Another provision that is aimed at ensuring robustness and accuracy of AI systems might be particularly significant in tackling discriminations originated by structural *biases*. It concerns, in particular, machine learning systems, which sometimes slip away from the protection granted by the GDPR. The AI Act requires that they should be developed in such a way to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations ('feedback loops').[78]

Furthermore, with regards to the information that providers must share with users in a clear, concise and complete way pursuant to Article 13, including for example the characteristics, capabilities and limitations of performance of the high-risk AI system, they are practical to overcome the technical illiteracy that otherwise employers might claim to have.

To verify the compliance with all the legal requirements the providers should undergo a conformity assessment procedure, pursuant to Article 43, nevertheless, with regards to AI systems deployed in employment context, this procedure is only based on internal control of the providers, revealing one

[78] Article 15, par. 4, AI Act.

of the limitations of the proposed regulation.[79] Together with the conformity assessment, providers shall also establish and document a post-market monitoring system in a manner that is proportionate to the risks of the high-risk AI system, according to Article 72.

As it has already been stated *supra*, the only obligation for deployers (namely, employers) is set out in Article 26, whose wording has undergone several revisions in the course of the versions of the AI Act, while leaving unchanged the core of the provision, essentially limited to following the instructions supplied by the provider. In addition to this obligation, deployers-employers should also assign human oversight to persons with the necessary competence, training and authority, on the basis of the instructions of use, in order to monitor the operation of the high-risk AI system and inform the providers, where relevant. In performing such monitoring, they must suspend the use of the system where they find that it may result in a risk, under the meaning of Article 79, i.e. to health or safety or to fundamental rights. This event triggers the activation of the procedure pursuant to Article 79, determining the need for the market surveillance authority to evaluate the system and order the provider to undertake corrective actions and, eventually, withdraw the AI system from the market.

Another obligation for deployers that has proven to be resilient in the subsequent versions of the Regulation refers to the use of the information provided under Article 13 to carry out the DPIA. This provision is particularly noteworthy, since it is intended to create consistency between the AI Act and the GDPR, making it easier for employers to implement the DPIA.

The framework on the requirements for deployers-employers is, at last, completed with a ‘timid’ regulation of the collective dimension and of the involvement of social partners, whose lack in the architecture of the proposed AI Act was heavily criticised.[80] Indeed, Article 26, par. 7, explicitly requires employers to inform workers’ representatives as well as affected workers of the use of the high-risk AI system, before putting into service it or prior to their use in the workplace. However, for the procedure and rules regarding such participatory right, the Regulation refers to existing EU or national law. In this regard, it must be noted that the version of the AI Act with the suggested amendments by the EU Parliament was more ambitious, to the extent that it required the employers to consult workers representatives to reach an agreement.[81]

Notwithstanding the merit of the proposed regulation, it has been critically welcomed by scholars for several reasons. Firstly, it is criticized because it doesn’t adopt a sectoral approach, ignoring, as a consequence, the peculiar needs of the employment context.[82] Apart from the lack or, at least, the weakness of collective and union approach in the draft Regulation,[83] another critique concerned the

[79] Article 43, par. 2. On the limits of such provisions, *see* for instance: Aida Ponce Del Castillo: *The AI Regulation: entering an AI regulatory winter? Why an ad hoc directive on AI in employment is required.* European Trade Union Institute, 2021.

[80] Ponce del Castillo (2021) op. cit.; Veale–Borgesius (2021) op. cit.; De Stefano–Wouters (2022) op. cit.

[81] Article 29, par. 5a, Amendments adopted by the European Parliament on 14 June 2023, available at: https://tinyurl.com/bdzdwayw

[82] De Stefano–Wouters (2022) op. cit.; Ponce del Castillo (2021) op. cit.; Jeremias Adams-Prassl: Regulating algorithms at work: Lessons for a ‘European approach to artificial intelligence’. *European Labour Law Journal,* vol. 13., issue 1. (2022) 30–50.

[83] De Stefano: The EU Proposed Regulation on AI: a threat to labour protection? *Global Workplace Law & Policy,* 16 April 2021.

lack of individual rights,[84] which has been been compensated with the introduction of the right to lodge a complaint with a market surveillance authority[85] and the right to explanation[86]. The latter can be seen as a relevant completion of the protection provided by Article 22, GDPR, with an *ex-post* information right that may be used as a basis to enforce workers' rights, in case of violation. Nonetheless, the inherent fragility of such a right persists, given that there aren't 'internal' mechanisms of review in place following the receipt of the explanation, in contrast to what is instead envisaged in the PWD Directive.[87] On the contrary, the infringement of the AI act provisions is punished even more incisively, with fines up to 35 millions EUR or, if the offender is company, up to 7% of its total worldwide annual turnover for the preceding financial year, in cases of violations of Article 5, while, in the other circumstances, with fines up to 15 millions EUR or, if the offender is company, up to 3 % of its total worldwide annual turnover for the preceding financial year.

## 5. PWD addressing algorithmic discriminations: from transparency requirements to the involvement of workers representative

The patchy jigsaw related to AMSs is completed by the PWD, proposed in December 2021 by the European Commission with the aim of enhancing platform workers' working conditions and social rights, while contributing to the sustainable growth of digital labour platforms. The proposal has been endorsed by the EU Parliament on 24th April 2024,[88] after an agreement was finally reached by the Parliament and the Council in March, but it has catalysed attention in the labour law community from the outset.[89]

This regulatory instrument is the only one among the others examined in this contribution that focuses particularly on the employment context and on workers' rights, resulting in a peculiar framework that recognises the existence of the imbalance of powers between the parties and the importance of workers' representatives, thus, meeting one of the greatest concerns raised by the approach of the GDPR and the AI Act.

With regards to the structure of the proposed Directive, two distinct set of rules are provided. The first one is related with the misclassification issues (Chapter II) and is not relevant for the purpose

[84] Ponce del Castillo (2021) op. cit.; Veale–Borgesius (2021) op. cit.; De Stefano–Wouters (2022) op. cit.

[85] Article 85, AI Act.

[86] Article 86, AI Act.

[87] See infra.

[88] The latest version of the PWD, adopted by MEPs, is available at https://tinyurl.com/wc8nvuuf. The analysis of the present paper will be mainly based on this version that, at the time of writing, is awaiting the formal adoption by the Council.

[89] See among others: Marco Barbieri: Prime osservazioni sulla proposta di direttiva per il miglioramento delle condizioni di lavoro nel lavoro con piattaforma. *Labour & Law Issues,* vol. 7., issue 2. (2021) C.3-C.20; Carla Spinelli: La trasparenza delle decisioni algoritmiche nella proposta di Direttiva UE sul lavoro tramite piattaforma. *Lavoro Diritti Europa,* vol. 2. (2022) 1–15.; Aloisi–Potocka-Sionek (2022) op. cit.; Ilaria Purificato – Iacopo Senatori: The Position of Collective Rights in the "Platform Work" Directive Proposal: Commission v Parliament. *Hungarian Labour Law E-Journal,* vol. 1. (2023) 1–19.

of this contribution; while the second one is aimed at addressing the issue related with AMSs in the workplace (Chapter III), promoting transparency, fairness and accountability. [90]

This Chapter applies to AMSs deployed in digital labour platforms, which include automated monitoring systems[91] and/or automated decision-making systems,[92] and encompasses several rights which strengthen and complement the rights provided in the GDPR, increasing legal certainty regarding their interpretation in the context of platform work.[93]

As a matter of fact, with regards to the transparency requirements, the right to be informed of automated monitoring and decision-making systems and the right to explanation enshrined in Articles 9 and 11 have their roots in the GDPR. Still, the PWD in Article 6 further specifies and completes the information to be shared, including, for instance, the categories of data and parameters that the system considers and the grounds for decisions to restrict, suspend, terminate or refuse remuneration. Moreover, it provides a formal requirement for the information which should be included in a transparent, intelligible, and easily accessible document, using clear and plain language. It also includes among the subjects entitled to receive information workers' representative, as well as competent national authorities, even though the latter solely upon request.

The inclusion of these entities – that can be found also in other provisions of the PWD (such as in Article 8, Article 10, Article 13, Article 14, etc.) – is particularly significant and marks a step forward in the regulatory framework with a recognition of collective rights, which are extremely important in the employment context to reduce the information asymmetries and to balance the relationship between the parties.

As regards the collective dimension, in the transparency architecture of the PWD, autonomous importance is given to information and consultation rights, although they are applied solely to platform workers with an employment contract. However, the formulation of the provision of Article 13 can be qualified merely as a reference to the Framework I&C Directive,[94] as it simply states that information and consultation rights also cover decisions to adopt or introduce substantial changes in an automated

[90] It must be noted that the adopted text has been heavily watered down from the original text of the Proposal especially in Chapter II dedicated to the Employment Status. Indeed, the legal presumption has, in the current version, less stringent contours compared to the rigid criteria identified in the Proposal. *See* for a first comment on the new text Antonio Aloisi – Valerio De Stefano: 'Gig' workers in Europe: the new platform of rights. *Social Europe,* 16 March 2024, available at: https://tinyurl.com/3zbpzha6 (last access 30 March 2024), who have welcomed with favour the compromise text, despite the step backward.

[91] According to Article 2, par. 1, (8) PWD, automated monitoring systems are systems which "are used for, or support monitoring, supervising or evaluating the work performance of persons performing platform work or the activities carried out within the work environment, including by collecting personal data, through electronic means".

[92] According to Article 2, par. 1, (9) PWD, automated decision making systems are systems which "are used to take or support, through electronic means, decisions that significantly affect persons performing platform work, including the working conditions of platform workers, in particular decisions affecting their recruitment, access to and organisation of work assignments, their earnings including the pricing of individual assignments, their safety and health, their working time, their access to training, promotion or its equivalent, their contractual status, including the restriction, suspension or termination of their account."

[93] Gaudio (2024) op. cit. 19.; Aloisi–Potocka-Sionek (2022) op. cit. In disagreement with this view: Ponce del Castillo–Naranjo (2022) op. cit.

[94] Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community.

monitoring system or decision-making system, subjects implicitly included in the material scope of the Framework I&C Directive.[95]

The direct involvement of workers' representatives also encompasses enforcement rights, to which individuals workers are entitled as well. Indeed, Article 11 provides platform workers and persons performing platform work with the right to receive an explanation for any decision taken or supported by an automated decision-making system.[96] Such right of explanation is also accompanied by a right to request the digital labour platform to review the decisions and an obligation to rectify it without delay when it is found to infringe the rights of persons performing platform work. There is consensus on the fact that the information rights, together with the explanation rights, establish the substance of remedial mechanisms triggered by allegedly discriminated workers, increasing their awareness, supporting the collection of evidence, and overcoming the 'opacity' issue.[97] Within the remedial measures available for workers' representatives, PWD also requires MS to ensure legal standing to those actors on behalf or in support of one or several persons performing platform work, in case of infringement of any right or obligation arising from the Directive, pursuant to Article 19.

In this regard, the directive also reinforces the investigatory powers of the judges in proceeding regarding the provisions of the directive, with the possibility to order to disclosure of any relevant evidence under their control as well as of evidence containing confidential information, if relevant for the proceeding, [98] supporting once again the opening of the 'black-box' and boosting strategic litigation.

The PWD also intensifies the preventive function of the GDPR with respect to discriminatory risks entailed by AMSs, with an approach even more incisive than the one adopted in Articles 9 and 22, GDPR. First of all, the human oversight is always required under Article 10, without any exceptions and not only in cases of solely automated decision making. In this regard, digital labour platform with the involvement of workers' representative shall oversee and assess regularly, and in any event every two years, the impact of individual decisions taken or supported by AMSs decision-making, most notably, with regard to their the discriminatory risks. To this end and in order to give efficacy to this requirement, the digital labour platforms, according to the PWD, should have sufficient human resources with the competence, training and authority needed to perform this task. Besides, the regular assessment provided under Article 10 is also considered to be more useful in fostering actual transparency, since most of the time examining the code of an algorithmic system does not provide

[95] Article 4, par. 2, (c): "(c) information and consultation on decisions likely to lead to substantial changes in work organisation or in contractual relations".

[96] With regards to the right to explanation, there is a contradiction in the GDPR, since it doesn't include it in Article 22, but it encompasses it in the Recital 71. On this concern, there is a considerable literature: Sandra Wachter – Brent Mittelstadt – Luciano Floridi: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. Rochester. *Social Science Research Network,* (2016) 10.; Edwards–Veale (2017) op. cit.

[97] Aloisi–Potocka-Sionek (2022) op. cit. 40.; Gaudio (2022a) op. cit.

[98] Article 21, PWD.

much useful information.[99] Additionally, transparency as a form of measurement on the impact of automated decision-making opens spaces for the correction of unequal or discriminatory conduct. Indeed, as required by Article 10, par. 3, PWD, in the occurrence of risks, the digital labour platform shall take the necessary steps including, if appropriate, a modification of the automated monitoring and decision-making system or a discontinuance of its use, in order to avoid such decisions in the future. This procedure, hence, influences the design of the AMS. Secondly, the PWD identifies a list of decisions which, given their significant detrimental legal effect, should not be taken at all by automated decision-making systems and, instead, must always be taken by a human being.[100] This list includes decisions to apply disciplinary measures, such as restricting, suspending or terminating the contractual relationship and the platform worker's account, or any decision of equivalent detriment, that could be potentially taken by AMSs. It should be noted that this provision is the result of the amendments of the European Parliament, and that in the opinion of the author it may result in a technological determinism. Thirdly, the area of exclusion of processable personal data is broader in Article 7 PWD, compared to GDPR, since the restriction is not limited to sensitive data alone,[101] but also includes data on emotional or psychological state; data in relation to private conversation, including conversations with workers' representatives; data collected outside the performance of work; data to predict the exercise of fundamental rights, including collective rights; and, lastly, any biometric data. Furthermore, these prohibitions are more stringent than those provided within the GDPR due to the absence of exceptions or derogations, as well as their wider scope of application, not limited to 'totally' automated decision making. Lastly, the consistency with the GDPR is also provided by Article 8, which explicitly mandates digital labour platform to carry out the DPIA, whose benefits with regards to the prevention of discrimination and the legibility of the algorithm have already been explained *supra*. In particular, the PWD requires platforms to take in consideration the opinion of workers' representatives, when implanting the DPIA.

From this preliminary investigation of the PWD it may be characterised as a *lex specialis* of the GDPR, intensifying protections especially in the realm of data processing, which hold significance in the era of data-driven decisions, while also completing the fragmentary legislative framework, adding consistency to it and – potentially – preventing discrimination effectively, from the very beginning, thanks to a reinforcement of transparency, an overall increase in the awareness of workers and a consideration of the collective dimension, as well as acting as a measure to support the gathering of evidence unveiling the truth hidden behind the algorithmic opacity.

[99] Borgesius (2020) op. cit. 1583.

[100] Recital 49 and Article 10, par. 5, PWD.

[101] Namely, racial or ethnic origin, migration status, political opinions, religious or philosophical beliefs, disability, state of health, including chronic disease or HIV status, the emotional or psychological state, trade union membership, a person's sex life or sexual orientation.

Still it has an important limitation. The PWD, indeed, has a very limited scope, since it only refers to AMSs deployed by digital labour platforms to manage platform workers or persons performing platform work. These workers, when the Directive will come into force, will result in having more protection than standard employees, even though the latter are subjected to AMSs as well. Hence, it represents a missed opportunity for the EU policymakers to govern the technology and stop constantly chasing it.

## 6. Conclusive remarks

The joint analysis of the GDPR, the AI Act, and the PWD, carried out in the previous sections in search for legal instruments suitable to tackle algorithmic discrimination and to support the non-discrimination legal framework, has shown that each of these regulatory instruments, despite of its shortcomings, provides some forms of protection against discriminations and, indirectly, addresses some of the limitations acknowledged in the antidiscrimination law.

Undoubtedly, the GDPR builds a robust architecture particularly devoted to the prevention of algorithmic discrimination, thanks to the transparency requirements, the prohibition to process sensitive data, and the duty to carry out a DPIA. These legal requirements, together with the contribution derived from the AI Act and the PWD, once they will come into force, will further reinforce the preventive function, for instance, ensuring that the criteria of the quality of data is met, as required by the AI Act, and thanks to the regular impact assessment, provided by Article 10, PWD. Thus, the validation of the AMSs and its impact will not just be limited to an *ex-ante* assessment, as provided especially by the AI Act with the conformity assessment and also by the GDPR with the DPIA, instead, it will follow the life-cycle of the system, thanks to the post-market monitoring system and impact assessment, resulted respectively by the implementation of AI Act and the PWD.

Furthermore, as it has been stated in the previous sections, the transparency requirements, which are recurring in all the legal sources analysed underlining the importance to address the information asymmetries, are especially meaningful also to reinforce the litigation strategies, promoted thanks to the legal opportunity structure inherent of non-discrimination law, since they open the algorithmic black box and help in the collection of the *prima facie* evidence to prove the existence of a discriminatory treatment in antidiscrimination claims. These transparency requirements vary in each statutory act and yet they complement each other. For instance, even though the AI Act doesn't encompass convincing duties on employers, it provides there-in an information duty from the providers to the deployers-employers, which, in turn, might be particularly helpful for employers to perform the DPIA and to obtain relevant information to share with the employees.

Aside from a specific investigation of the significant limitations that each regulatory instruments has and which have already been acknowledged in each Section, the optimistic aim of this contribution has been instead to foster the awareness of the potentiality of other – existing or in progress – legal measures to address the rise of algorithmic discriminations with the final goal to ensure that these laws are better known, actually complied with, and, in the end, more effective, thanks to a combined exercise of these rights.

In the end, rather than conceiving AMSs as a threat to objectivity and neutrality, they may also represent an opportunity to correct biases already happening in humans' mind and yet opaque and not explicit. Perhaps, to face the rise of algorithmic discrimination, we just need a new and more solid strategy that may be supported by the interplay of these regulatory instruments in order to ensure that these regimes become mutually reinforcing and complementary in the workplace.