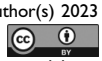
Check for updates

Special Issue Contribution

ELLJ

European Labour Law Journal
2023, Vol. 14(2) 283–307
© The Author(s) 2023

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20319525231167982
journals.sagepub.com/home/ell


Between risk mitigation and labour rights enforcement: Assessing the transatlantic race to govern AI-driven decision-making through a comparative lens

Antonio Aloisi
IE University Law School, Madrid, Spain

Valerio De Stefano
Osgoode Hall Law School, York University, Toronto, Canada

Abstract

In this article, we provide an overview of efforts to regulate the various phases of the artificial intelligence (AI) life cycle. In doing so, we examine whether—and, if so, to what extent—highly fragmented legal frameworks are able to provide safeguards capable of preventing the dangers that stem from AI- and algorithm-driven organisational practices. We critically analyse related developments at the European Union (EU) level, namely the General Data Protection Regulation, the draft AI Regulation, and the proposal for a Directive on improving working conditions in platform work. We also consider bills and regulations proposed or adopted in the United States and Canada via a transatlantic comparative approach, underlining analogies and variations between EU and North American attitudes towards the risk assessment and management of AI systems. We aim to answer the following questions: Is the widely adopted risk-based approach fit for purpose? Is it consistent with the actual enforcement of fundamental rights at work, such as privacy, human dignity, equality and collective rights? To answer these questions, in section 2 we unpack the various, often ambiguous, facets of the notion(s) of 'risk'—that is, the common denominator with the EU and North American legal instruments. Here, we determine that a scalable, decentralised framework is not appropriate for ensuring the enforcement of constitutional labour-related rights. In addition to presenting the key provisions of existing schemes in the EU

Corresponding authors:
Antonio Aloisi, Assistant Professor, IE University Law School, Madrid.
Email: antonio.aloisi@ie.edu.

Valerio De Stefano, Canada Research in Innovation, Law and Society, Osgoode Hall Law School, York University, Toronto.
Email: vdestefano@osgoode.yorku.ca.

and North America, in section 3 we disentangle the consistencies and tensions between the frameworks that regulate AI and constrain how it must be handled in specific contexts, such as work environments and platform-orchestrated arrangements. Paradoxically, the frenzied race to regulate AI-driven decision-making could exacerbate the current legal uncertainty and pave the way for regulatory arbitrage. Such a scenario would slow technological innovation and egregiously undermine labour rights. Thus, in section 4 we advocate for the adoption of a dedicated legal instrument at the supranational level to govern technologies that manage people in workplaces. Given the high stakes involved, we conclude by stressing the salience of a multi-stakeholder AI governance framework.

Keywords
artificial intelligence, risk-based approach, algorithmic management, platform work, automated decision-making, data protection, impact assessment, comparative analysis

1. Introduction

In recent years, workers in all industries have become inexorably acquainted with a set of human resource practices partially 'outsourced' to digital devices and software that rely on artificial intelligence (AI) to optimise processes, enhance efficiency, and minimise costs.[1] Moreover, managerial functions can be performed, or at least supported, by data-driven tools across the entire range of contractual phases, from recruitment to termination, task administration to performance assessment. Numerous accounts have detailed how hiring procedures are now completed online and processed by algorithms,[2] while prerogatives such as scheduling shifts, forecasting personnel requirements and allocating assignments can equally now be offloaded to online applications with relative ease and speed. To nurture these new functions, worker monitoring is constantly and ubiquitously performed, thanks to the virtually infinite set of data-capturing and -processing systems currently available, and the large-scale information derived provides management with granular knowledge that informs both day-to-day and real-time decision-making.

Popular awareness of so-called 'algorithmic bosses' is increasing,[3] and not without reason. Several traditional guardrails are at risk of being unsettled due to how these systems are conceived and operated. First, they are able to collect and elaborate huge swathes of data almost instantaneously and from multiple sources, due to their seemingly infinite scalability, and they can do so without the observed being cognisant of the tracking. Second, once instructed to pursue a particular objective by their designers and deployers, algorithmic models are unbeatably efficient, 'mechanistic', and mission-oriented,[4] meaning that they fail to consider any exceptions. Third, as they are being adopted within a far-from-perfect social fabric, they end up calcifying biases, inequalities,

1. Tammy Katsabian, 'Managerial "Outsourcing" in the Digital Reality and its Implications on the Right to Equality' (IE Lawtomation Days, Madrid, 29 and 30 September 2022).
2. Ifeoma Ajunwa, 'The "Black Box" at Work' (2020) 7(2) Big Data & Society 1.
3. Jodi Kantor and Arya Sundaram, 'The Rise of the Worker Productivity Score' *New York Times* (New York 15 August 2022) <https://nyti.ms/3B8l7sV> accessed 10 April 2023.
4. Andrew D Selbst, 'An Institutional View of Algorithmic Impact' (2021) 35 Harvard Journal of Law & Technology 117.

and stereotypes, despite being erroneously depicted as a silver bullet with which to overcome shortcomings known to plague analogue reality, such as inefficiencies, disparities, inaccuracies, and arbitrariness. To complicate things further, existing redress mechanisms, which are designed to address a different form of authority, are not equipped to curb the inaccuracies and abuses of algorithms.

Aside from being a distinctive feature of digital labour platforms' business model,[5] automated decision-making has also been widely adopted in almost all sectors in which data represent the underlying infrastructure (e.g., warehouses, home offices, stores, factories, and consulting companies).[6] Due to being confronted with an ever-evolving set of potential promises and risks, lawmakers worldwide are pondering whether to step in and seek to better regulate this growing trend. For instance, the European Union (EU) institutions have proposed a panoply of intertwined regulatory measures that display integrated or overlapping characteristics. Yet, the relationship between these initiatives is intricate and contentious. For example, while solely automated decision-making on the basis of personal data is thoroughly regulated by the General Data Protection Regulation (GDPR) and similarly, albeit more narrowly, covered in the context of digital labour platforms by the proposal for a Directive on improving working conditions in platform work (Platform Work Directive [PWD]), the draft AI Regulation classifies some AI-driven practices in the employment context as high risk and then simply defines procedural steps that providers must comply with to ensure their 'conformity' with certain requirements.[7] A comparable trend of policy activism and stratification can be seen in both the United States (e.g., the NIST Artificial Intelligence Risk Management Framework and the Algorithmic Accountability Act) and Canada (e.g., the Artificial Intelligence and Data Act).

Without engaging with the taxonomical quandary that surrounds the notions under scrutiny, we rely on (still contested) institutional definitions. Here, AI refers to 'systems that display intelligent behaviour by analysing their environment and taking actions—with some degree of autonomy—to achieve specific goals'.[8] In the draft AI Regulation (which is also known as the AI Act), AI systems are defined as software that 'can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with' (Article 3).[9] The latter definition considers the overarching roles played by AI, such as 'improving prediction, optimising operations and resource allocation, and personalising digital solutions

5. European Commission, 'Impact Assessment Report accompanying the document Proposal for a Directive of the European Parliament and of the Council to improve the working conditions in platform work in the European Union' SWD(2021) 396 final/2, Annex A11.2.
6. Antonio Aloisi and Valerio De Stefano, *Your Boss is an Algorithm: Artificial Intelligence, Platform Work and Labour* (Hart Publishing, 2022).
7. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (22 April 2021) (AI Act). See Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act—Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 Computer Law Review International 97.
8. European Commission High-Level Expert Group on Artificial Intelligence, 'A Definition of AI: Main Capabilities and Scientific Disciplines' COM (2018) 237 final.
9. For a similar definition, see Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council on Artificial Intelligence* (OECD 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 10 April 2023 ('a machine-based system that can, for a given set of human defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments').

available for individuals and organisations' (Recital 3). By contrast, in the proposed PWD, automated decision-making systems are identified by reference to their functions, namely 'to take or support decisions that significantly affect workers' working conditions'.[10] Similarly, algorithmic management can be conceptualised as the use of 'software to automate organisational functions traditionally carried out by human managers, identified in both platform work and conventional employment settings'.[11]

Underpinning most recent regulatory efforts is the increasingly important notion of 'risk', which has risen to sit among the prominent organising principles of today's complex reality, despite the discord among experts concerning its meaning.[12] The 'risk-based model' embodies a modern regulatory attitude[13] and offers a method for furthering compliance in highly technical sectors in which fully prescriptive regulation is unable to keep pace with new developments.[14] From the outset, it must be noted that risk functions as a yardstick for the interpretation, 'calibration', and application of legal norms, thereby going beyond the classical 'top-down' and 'one-size-fits-all' methodologies.[15] Indeed, inspired by product safety legislation, the risk-based approach necessitates a shift towards a 'granular, scalable' logic[16] that is often not compatible with fundamental rights enforcement.[17] The model's operation is dependent on the context in which it is applied,[18] and it involves at least two main phases. The first phase ('assessment') is devoted to forecasting the likelihood and severity of a certain event, whereas the second phase ('management') involves the implementation of coordinated mitigation activities intended to reduce the risk to the point where 'the harms do not outweigh the benefits and the risk is deemed sufficiently low to be taken'.[19]

This article sketches an overview of recent regulatory attempts to address the different stages of the AI life cycle—that is, the interconnected series of consecutive steps that enable the functioning of such systems. In doing so, it examines whether—and, if so, how—highly fragmented regulatory

10. Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM (2021) 762 final (9 December 2021) (Platform Work Directive [PWD]), art 6(1).
11. Alex J Wood, 'Algorithmic Management Consequences for Work Organisation and Working Conditions' (2021) JRC Working Papers Series, WP No 7; Sara Baiocco, Enrique Fernández-Macías, Uma Rani, and Annarosa Pesole, 'The Algorithmic Management of Work and its Implications in Different Contexts' (European Commission 2022); Katherine C Kellogg, Melissa A Valentine and Angèle Christin, 'Algorithms at Work: The New Contested Terrain of Control' (2020) 14 Academy of Management Annals 366.
12. Alberto Alemanno, 'Regulating the European Risk Society' in Alberto Alemanno, Frank AG den Butter, Andre Nijsen, and Jacopo Torriti (eds), *Better Business Regulation in a Risk Society* (Springer 2012) 37–56 (describing risk as a novel '*Grundnorm*'); Ulrich Beck, *Risk Society, Towards a New Modernity* (SAGE Publications Ltd 1992).
13. Michael Power, *The Risk Management of Everything—Rethinking the Politics of Uncertainty* (Demos 2004).
14. Tobias Mahler, 'Between Risk Management and Proportionality: The Risk-based Approach in the EU's Artificial Intelligence Act Proposal' (2021) Nordic Yearbook of Law and Informatics 258.
15. AI Act Recital 14.
16. Raphael Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-based and the Risk-based Approaches to Data Protection' (2016) 2 European Data Protection Law Review 481.
17. Niklas Jedrzej and Lina Dencik, 'What Rights Matter? Examining the Place of Social Rights in the EU's Artificial Intelligence Policy Debate' (2021) 10(3) Internet Policy Review 1.
18. Aislinn Kelly-Lyth and Anna Thomas, 'Algorithmic Management: Assessing the Impacts of AI at Work' (elsewhere in this issue); see also Pietro Dunn and Giovanni De Gregorio, 'The Ambiguous Risk-Based Approach of the Artificial Intelligence Act: Links and Discrepancies with Other Union Strategies' (CEUR Workshop Proceedings, 2022).
19. A third phase is identified in 'communication'. Gellert (n 16). See also International Organization for Standardization (ISO) standard 31000 <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en> (on the process of risk identification, analysis and evaluation).

frameworks can offer reliable safeguards that prevent the harms stemming from AI- and algorithm-driven organisational practices. Moving beyond a labour law perspective and embracing a law and governance approach, we intend to answer the following research questions: Is the widely adopted risk-based methodology fit for purpose? Is it consistent with the actual enforcement of fundamental rights at work, such as privacy, human dignity, equality, and collective rights? We look at developments at the EU level to retrace the consistency and tensions between related tools. Moreover, we also evaluate bills, regulations and soft law tools proposed or adopted in the United States and Canada using a transatlantic (functionalist) comparative approach,[20] underlining the analogies and differences between EU and North American attitudes to risk assessment and management.

The remainder of this article is structured as follows. Section 2 focuses on the notion(s) of 'risk' as the common denominator in some EU and North American legal instruments, with the aim being to unpack its various, often nebulous, connotations. We contend that a scalable governance framework, which is partially outsourced to those entities targeted by the relevant regulation, is not appropriate for ensuring compliance with the fundamental rights chiefly impacted by AI- or algorithm-driven practices. In addition to presenting the key provisions of the existing legal schemes, section 3 highlights their interactions as well as the antinomies that exacerbate legal uncertainty and pave the way for regulatory arbitrage. Paradoxically, this frenzied race to regulate AI could slow technological innovation, undermine national frameworks regulating the introduction of workplace technologies, and erode fundamental rights. Finally, Section 4 discusses whether professional settings deserve a dedicated instrument, given both the high stakes involved and the pre-existing power structures. In light of this discussion, the article concludes by stressing the importance of a collective AI governance framework that involves those individuals and communities affected during the design, development and deployment phases.

2. Navigating the ambiguity of 'risk' and the pitfalls of risk-based regulation

2.1. Approaches to regulating AI through risk in the EU, United States, and Canada

In this section, we analyse the multiple connotations of the notion of risk in certain EU regulatory instruments (the AI Act, the GDPR, and the PWD, in order of the amount of discussion) and compare them with North American instruments.[21]

The Explanatory Memorandum drafted by the European Commission explicitly states that the AI Act 'puts in place a proportionate regulatory system centred on a well-defined risk-based regulatory approach that does not create unnecessary restrictions to trade'.[22] Moreover, 'legal intervention is tailored to those concrete situations where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future'. The AI Act pursues four main goals (although this succession of priorities is not reflected in the substantive sections of the Act):

20. Ralf Michaels, 'The Functional Method of Comparative Law' in Mathias Reiman and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press 2006).
21. Niels Van Dijk, Raphaël Gellert, and Kjetil Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286; see also Jacqueline Peel, *Science and Risk Regulation in International Law* (Cambridge University Press 2010).
22. European Commission, 'Explanatory Memorandum to the AI Act Proposal' COM(2021) 206 final, 3.

(i) guaranteeing that AI systems are safe and respect fundamental rights and values;
(ii) ensuring legal certainty to facilitate investment and innovation;
(iii) enhancing governance and the effective enforcement of fundamental rights and the safety requirements for AI systems; and
(iv) facilitating the development of a single market for lawful, safe, and trustworthy AI, thereby preventing fragmentation and regulatory arbitrage.

The EU Commission did not want to introduce any unnecessary costs that would slow the race to develop AI, although they recognised the need to design effective supervision and enforcement mechanisms in order to avoid infringements of fundamental rights and breaches of safety.

A proactive model both empowers AI 'developers' and shifts the burden of compliance (and the associated mandatory reporting) onto them. The AI Act lays down specific rules under Title III—that is, the 'core' of the Regulation.[23] AI systems that 'create a *high risk* to the health and safety or fundamental rights of natural persons' encompass the components of products that are subject to *ex-ante* conformity assessments conducted by sectoral regulators (e.g., toys, machinery, or medical equipment) and 'other stand-alone AI systems with mainly fundamental rights implications' as listed in the updatable yet rigid Annex (while new subcategories can be added, the main categories cannot be altered). AI systems are permitted provided they comply with certain essential requirements and pass the conformity assessments and reviews performed by the 'providers', who are considered to be best placed to gauge the risks posed by their AI systems.[24] Less involvement is required on the part of users,[25] who, in the context of work, would almost always be employers. This clearcut distinction does not take into account the dynamic nature of AI development, deployment and monitoring or the possibility of 'co-production', whereby users participate in the design of AI systems.[26]

The high-risk AI systems referred to in Article 6(2) of the AI Act are made explicit in Annex III. Tellingly, among these 'highly risky' systems are those adopted in the context of 'employment, workers management and access to self-employment' (point 4) that must undergo the conformity assessment procedure prior to entering the market or being put into service. In particular, reference is made to:

(a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, or evaluating candidates in the course of interviews or tests; and
(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation, and for monitoring and evaluating performance and behaviour of persons in such relationships.

23. Aída Ponce Del Castillo, 'The AI Regulation: Entering an AI Regulatory Winter?' (ETUI Policy Brief, July 2021).
24. A similar model can be found in European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on machinery products' COM (2021) 202 final.
25. Or, to borrow a broad definition proposed by Edwards, 'deployers'. Lilian Edwards, *Regulating AI in Europe: Four Problems and Four Solutions* (Ada Lovelace Institute, 2022) <https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/#fn-8> accessed 10 April 2023. According to the draft, the AI Act provisions affecting the world of work also apply to the self-employed, meaning that they cover entities or people that, at least theoretically, are not technically 'employers'.
26. Norberto Nuno Gomes de Andrade and Antonella Zarra, *Artificial Intelligence Act: A Policy Prototyping Experiment: Operationalizing the Requirements for AI Systems – Part I* (Open Loop 2022).

In short, while the list of functions is neither comprehensive nor exhaustive, the Annex captures some of the most common uses of AI in the work context—that is, functionally and logically interconnected human resource practices that 'may appreciably impact future career prospects and livelihoods of these persons' (Recital 36).

A provider is 'a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge' (Article 3 of the AI Act).[27] It is up to the provider to specify the purpose of an AI system, which then determines its classification and the consequent obligations under Article 16. The classification considers the intended purpose of an AI system and the modalities for which it is used. Despite the aim of delivering a modular and targeted framework, AI technologies are classified in an 'abstract' and 'context-neutral' manner within the AI Act,[28] with no consideration of case-specific uses. A key limitation of the Regulation is the fact that it fails to consider the multipurpose and adaptive nature of AI systems, which can be easily re-coded and 'employed for completely different purposes from those for which they were designed'.[29] Aside from the developers' duty to consider and mitigate the risks stemming from 'reasonably foreseeable misuse',[30] this process only barely addresses what experts term 'function creep', which involves the progressive widening of the use of systems beyond the purposes for which they were originally intended.

According to Article 9 of the AI Act, the providers of high-risk AI systems must establish, implement, document, and maintain a risk management system throughout the life cycle of a given AI system. In this complex architecture, high-risk AI systems are permitted so long as a 'continuous iterative process' is put in place and systematically updated (Article 9(2)). The providers are required to identify and analyse the 'known and foreseeable risks' as well as to evaluate the 'risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse'. They must also evaluate other 'risks based on the analysis of data gathered from the post-market monitoring system' and, notably, adopt 'suitable risk management measures'. Within this margin of appreciation, the providers can assume necessary risk mitigation strategies and deploy internal controls based on the verification of the quality management system, examination of the information included in the technical documentation (a form of user transparency),[31] and verification of the consistency between the design and development process of the relevant AI system and the technical documentation provided.[32]

27. According to Article 28 of the AI Act, distributors, importers, users, or other third parties shall be considered a provider for the purposes of the Regulation when they (a) 'place on the market or put into service a high-risk AI system under their name or trademark', (b) 'modify the intended purpose of a high-risk AI system already placed on the market or put into service' or (c) 'make a substantial modification to the high-risk AI system'.
28. Martin Ebers, 'Standardizing AI: The Case of the European Commission's Proposal for an Artificial Intelligence Act' in Larry A Di Matteo, Cristina Poncibò, and Michel Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press 2022).
29. Vera Lúcia Raposo, 'The European Draft Regulation on Artificial Intelligence: Houston, We Have a Problem' in EPIA Conference on Artificial Intelligence (Springer 2022) 68; see also Alessandro Mantelero and Maria Samantha Esposito, 'An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems' (2021) 41 Computer Law & Security Review 7.
30. For a more in-depth discussion, see Miriam Kullmann and Aude Cefaliello, 'The Draft Artificial Intelligence Act (AI Act): Offering False Security to Undermine Fundamental Workers' Rights' (2022) 13(4) European Labour Law Journal 7.
31. Veale and Zuiderveen Borgesius (n 7) 12.
32. AI Act, Annex VI.

The risk-based model is not exclusive to the AI Act. A similar, albeit more open-textured, approach also informs the GDPR. Under Article 35 of the GDPR,[33] when data processing involving technologies 'is likely to result in a high risk to the *rights and freedoms* of natural persons',[34] the data controller (who is generally the employer) must preventively 'carry out an assessment of the impact of the envisaged processing operations on the protection of personal data'. Any discrimination stemming from algorithmic management, as one common example in this regard, falls neatly within this risk-centred model.[35] This type of risk assessment is required when personal aspects related to natural persons are systematically and extensively evaluated by means of automated processing, including profiling, that results in decisions with legal or similarly significant effects. According to Article 35(7) of the GDPR, the assessment must include the description of the operations and purposes of the processing, clarification of necessity and proportionality, and elucidation of both the risks faced by the data subjects (workers) and the measures adopted to address those risks and demonstrate compliance with the GDPR.[36]

Moreover, given the 'nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons', Article 24(1) of the GDPR imposes on the data controller the duty to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate' that the relevant data processing is performed in accordance with the GDPR. Relatedly, Article 25(1) of the GDPR fleshes out an employer's duty to effectively 'implement appropriate technical and organisational measures' and 'integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects'. This must be done after conducting a specific risk assessment, both prior to and during the data processing, which considers 'the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'.

33. Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations' (2020) 11 International Data Privacy Law 125; Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754; Katerina Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of "high risk" in the General Data Protection Regulation' (2019) 35 Computer Law & Security Review 105342.
34. Emphasis added. Recital 75 explains that the risk 'may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination . . . or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms . . ; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership . . . where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work'.
35. Antonio Aloisi, 'Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights' (2024) 40(1) International Journal of Comparative Labour Law and Industrial Relations 1.
36. A Data Protection Impact Assessment is required when 'compan[ies] systematically monitor employees' activities, including . . . work station, internet activity, etc.' Article 29 Working Party, '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) WP 248 rev.01.

The notion of risk is operationalised within the GDPR by means of 'meta-obligations'[37] in such a way as to render data controllers (or employers, for the purpose of our analysis) responsible and accountable.[38] The need to fulfil such general requirements is expected to serve as a compliance-enhancing method. As a consequence, provided that all of the GDPR principles are respected, data controllers can modulate their regimes by assessing the likelihood and intensity of the envisaged risk of the related processing operations, rather than having to comply with a highly standardised model.[39] The determination of the level of risk, the resulting salience of putting into place mitigation strategies, and the identification of technical and organisational measures represent part of a 'knowledge gathering and analysis' phase that is left to the employers themselves.[40] Employers also enjoy a discrete margin of appreciation with regard to the identification of the most appropriate technical and organisational measures (Article 5 of the GDPR).

When reading the fine print, it becomes apparent that a similar scheme is replicated within (the original version of) the proposed Platform Work Directive. In particular, under Article 7 of the PWD, a *sui generis* algorithmic impact assessment of the risks associated with automated monitoring and decision-making systems when it comes to the occupational safety and health (OSH) of platform workers is introduced. However, the framing of this instrument is indirect—that is, Member States (MS) have a duty to compel digital platforms (in their role as employers or principals) to 'regularly monitor and evaluate the impact of individual decisions taken or supported by automated monitoring or decision-making systems' (Article 7(1)). In addition, platforms must put in place a reliable mechanism supported by 'sufficient human resources' responsible for compliance with the rules laid down in the national laws transposing the PWD (Article 7(3)). We have commented elsewhere that the key limitation of the approach adopted in the PWD lies in the uncritical acquiescence to the introduction of such highly invasive organisational patterns, which have already proven to undermine workers' agency and erode the workers' experience of their job.[41]

When it comes to OSH, digital platforms are required to (i) conduct a risk assessment, 'in particular as regards possible risks of work-related accidents, psychosocial and ergonomic risks'; (ii) assess whether the current safeguards are suitable for addressing the risks identified, considering the work environment; and (iii) adopt appropriate preventive and protective measures (Article 7(2)). Moreover, automated monitoring and decision-making processes must not increase the pressure or augment the health-related risks faced by platform workers (a similar requirement can be found in California Assembly Bill 701, as discussed below). This is a rather narrowly specified 'human monitoring' procedure, which must be read in conjunction with the risk assessment required by the GDPR. Given the inclusion within a set of provisions that (also) apply to self-

37. Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 European Journal of Risk Regulation 502. These provisions trigger a multidimensional process whose ownership in terms of interpretation and application of the GDPR safeguards resides entirely with the data holders. See also Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave, and Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press 2010) 146.
38. Reuben Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 International Data Privacy Law 22.
39. Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (22 August 2018) WP 251 rev.01, 19.
40. Quelle (n 37).
41. Valerio De Stefano, 'The EU Commission's Proposal for a Directive on Platform Work: An Overview' (2022) 15 Italian Labour Law E-Journal 1.

employed persons performing platform work, it is odd that the rights pertaining to health and safety at work are reserved for 'workers in view of Union law' (Recital 40). The second section of the same Article has a broader ambit that also encompasses genuinely self-employed workers, whereas only 'workers' fall within the scope of Articles 7(1) and (3).

Across the Atlantic, the National Institute of Standards and Technology (NIST), part of the United States Department of Commerce, takes a similar approach. In March 2022, it introduced a voluntary framework, the NIST Artificial Intelligence Risk Management Framework (AI RMF),[42] intended to improve the management of risks stemming from AI and affecting individuals, organisations, and society in general. The framework is designed to deploy a flexible, outcome-focused, cost-effective approach to the design, development, use, and evaluation of AI products, services, and systems. As detailed in the document that launched the multi-stakeholder consultation, 'managing' means identifying, assessing, responding to, and communicating the risks of AI. The draft focuses on technical characteristics (accuracy, reliability, robustness and resilience), socio-technical characteristics (explainability, interpretability, privacy, safety, and managing bias) and guiding principles (fairness, accountability, and transparency).[43] It also defines risk as 'a measure of the extent to which an entity is negatively influenced by a potential circumstance or event [considering] 1) the adverse impacts that could arise if the circumstance or event occurs; and 2) the likelihood of occurrence'[44] and designs a three-part solution based on mapping, measurement, and management. However, despite the abundance of procedural safeguards, the framework lacks binding force.

In addition, while there is nothing akin to the EU's 'horizontal' approach, a comparable scheme geared towards mandatory impact assessments regarding AI use is currently making its way through Congress, namely the Algorithmic Accountability Act. The Bill was presented in 2021,[45] although no significant progress has been made since then. If approved, it would require the Federal Trade Commission (FTC) to develop regulations requiring large firms (which are defined as those with over USD 50 million in revenue or those that hold data concerning at least one million consumers or consumer devices) to conduct impact assessments in relation to existing and new 'high-risk automated decision systems' (including systems that 'analyze or predict sensitive aspects of [consumers'] lives, such as their work performance, economic situation, health, personal preferences, interests, behavior, location, or movements, [and] alter legal rights of, or otherwise significantly impact, consumers') and maintain relevant documentation. The systems that would fall within this category are those that may contribute to inaccuracy, bias, or discrimination, or those that facilitate decision-making regarding sensitive aspects of consumers' lives by evaluating individuals' behaviour. The Bill partially reproduces the logic of the AI Act and the

42. Information Technology Laboratory, 'AI Risk Management Framework: AI RFM 1.0' (January 2023) <https://www.nist.gov/itl/ai-risk-management-framework> accessed 10 April 2023.
43. Reva Schwartz et al, 'Towards a Standard for Identifying and Managing Bias in Artificial Intelligence' (National Institute of Standards and Technology Special Publication 1270, 2022) <https://doi.org/10.6028/NIST.SP.1270> accessed 10 April 2023.
44. AI Risk Management Framework: Initial Draft (n 42).
45. Algorithmic Accountability Act of 2019, HR 2231, 116th Cong (2019) (requiring certain commercial entities to conduct assessments of high-risk systems that involve personal information or make automated decisions). See also Lisa J Bernt, 'Workplace Transparency Beyond Disclosure: What's Blocking the View?' (2021) 105 Marquette Law Review 73; Jakob Mökander, Prathm Juneja, David S Watson, and Luciano Floridi, 'The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?' (2022) 32 Minds and Machines 751.

GDPR, establishing a model that delegates to developers the task of carrying out risk assessment and management practices.

In Canada, further corroborating the suggestion that we are currently living in the golden age of the risk-based approach, the Federal Government introduced Bill C-27 into Parliament in 2022. Bill C-27 includes the Consumer Privacy Protection Act (CPPA) and the Artificial Intelligence and Data Act (AIDA). The AIDA provides that 'a person responsible for a high-impact system', as defined within regulations, 'must, in accordance with [such] regulations, establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system'. Similar to the EU's AI Act, the AIDA adopts a risk-based approach. It is unclear at this stage if the regulations will eventually define systems that have implications for employment and occupation among the 'high-impact' ones, which contrasts with the approach of the EU's AI Act in defining such systems as 'high-risk'.[46]

2.2 Questioning the basic presuppositions of the risk-based approach to AI at work

Albeit to varying extents, the novel EU legal tools concerning AI, the American NIST AI RMF, and the Canadian AIDA all pursue the goal of trustworthy AI systems, which accords with the idea that a set of mandatory requirements renders opaque systems more 'reliable', thereby fostering end users' confidence in such instruments. One key difference is that the NIST AI RFM has a non-binding nature. Additionally, there are also minor differences among the risk-based approaches incorporated into the EU legislation. The GDPR and the PWD are hybrid frameworks.[47] They reflect an open-ended and bottom-up exercise that does not excessively constrain the room to manoeuvre of data controllers and digital labour platforms. While the AI Act model is rather more rigid in its classification of areas,[48] it provides a 'fast lane' reserved for AI providers, who are assigned a certain degree of subjectivity despite the mandatory conditions, which contrasts with the strict national regulation of issues such as workplace data collection and processing on the one hand and decision-making on the other.

Based on the above overview, it is clear that, despite its elusive and highly contested nature,[49] the risk-based approach is widespread in policymaking and predicated on the replacement of the 'formal legality and enforcement of individual rights' with a model of 'self-regulation for managing innovation in uncertain scenarios'.[50] When dealing with highly volatile matters, policymakers tend to prefer the use of adaptive techniques that are 'calibrated' to their targets in an attempt to avoid excessive constraints and paralysing effects on strategic and capital-intensive industries.[51] Such models are also conceived as 'assum[ing] a technology will be adopted despite its harms',[52]

46. Government of Canada, *Algorithmic Impact Assessment Tool* <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html> accessed 10 April 2023.
47. Kaminski and Malgieri (n 33).
48. Giovanni De Gregorio and Pietro Dunn, 'The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59 Common Market Law Review 473.
49. Power (n 13) 13–14.
50. Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-fold Shift' (2017) 8 European Journal of Risk Regulation 506.
51. Quelle (n 37).
52. Margot E Kaminski, 'Regulating the Risks of AI' (2023) 103 Boston University Law Review (forthcoming) <https://ssrn.com/abstract=4195066> 10 April 2023.

which is questionable. These models partially shift the responsibility onto those creating the potential risk-event and the (lower-end) regulatory prerogative onto decentralised agencies believed to be better positioned when it comes to gathering scientific evidence and ensuring contextual enforcement.[53] They are also consistent with the rules and principles of data protection,[54] which favour anticipatory and collaborative measures.

What should be said about the appropriateness of this method? The abandonment of prescriptive frameworks is alarming, especially when such systems affect human agency and dignity as they do in the context of work, among others. The danger is that non-waivable rules and principles in the workplace (from autonomy to respect for private life, decent wages and working time to non-discrimination, equality to freedom of expression and association)[55] will end up being sacrificed on the altar of a nebulous notion of 'compliance 2.0' comprised of cosmetic audits, vague checklists and courtesy toolkits.[56] As we detail in a forthcoming study, there is a stark discrepancy between a quantitative model of compliance, which is 'directed toward numerical assessments of the probability and severity of tangible harm',[57] and the logic of (immeasurable and unconditional) constitutional rights that cannot be toned down.[58] Any attempt to deliver risk mitigation strategies cannot overlook the 'sensitivity' of work environments, where an extra layer of substantive and procedural precautions is already required by national laws,[59] which often mandate the involvement of those who are subject to decisions. To this must be added the sheer lack of consideration of the social, collective, and human rights implications of this model,[60] a point that we shall return to in the final section of this article.[61]

53. Sofia Ranchordás, 'Experimental Regulations and Regulatory Sandboxes: Law without Order?' in Sofia Ranchordás and Bart van Klink (eds), *Law & Method* (BJu Legal Publishers 2021).
54. Raphael Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law 3; Gellert (n 16).
55. Charter of Fundamental Rights of the European Union OJ C326/391 (EU Charter). According to the Explanatory Memorandum, 'Consistency is also ensured with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality'.
56. For a similar perspective, see Fanny Hidvegi, Daniel Leufer, and Estelle Massé, 'The EU Should Regulate AI on the Basis of Rights, Not Risks' (*AccessNow*, 17 February 2021) <https://www.accessnow.org/eu-regulation-ai-risk-based-approach/> accessed 10 April 2023. See also Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' (30 May 2014) WP 218 ('. . . the Working Party is concerned that . . . the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles, rather than as a scalable and proportionate approach to compliance' and 'Fundamental principles . . . should remain the same, whatever the processing and the risks for the data subjects').
57. Karen Yeung and Lee A Bygrave, 'Demystifying the Modernized European Data Protection Regime: Cross-disciplinary Insights from Legal and Regulatory Governance Scholarship' (2022) 16 Regulation & Governance 143.
58. According to Article 52(1) of the EU Charter, limitations provided for by law are subject to the principle of proportionality and can be exercised only if they are necessary and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others. See also Lottie Lane, 'Clarifying Human Rights Standards Through Artificial Intelligence Initiatives' (2022) 71 International & Comparative Law Quarterly 915.
59. Phoebe Moore, 'Data Subjects, Digital Surveillance, AI and the Future of Work' (2020) European Parliamentary Research Services, Scientific Foresight Unit (PE 656.305). See also Aída Ponce Del Castillo, 'A Law on Robotics and Artificial Intelligence in the EU?' (ETUI Foresight Brief 02, 2017).
60. Alessandro Mantelero, 'Beyond Data' in Alessandro Mantelero (ed), *Beyond Data* (TMC Asser Press 2022) 27; Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754.
61. Lorna McGregor, Daragh Murray, and Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability' (2019) 68 International & Comparative Law Quarterly 309.

3. Transatlantic insights: Legal transfers and headlong rushes

3.1 More (regulation) is less (protection)? The increasingly patchy EU framework

To paint as accurate a picture as possible, it must be noted that the EU institutions are both championing innovative regulation and grappling with its potential unintended consequences. The accretion of partially intersecting and diverging measures is not limited to the risk assessment models documented in the previous section. Researchers have begun to explore the startling 'overlaps, gaps and inconsistencies' in the 'patchwork' of regulation, including between the newly proposed AI Act and existing legislation,[62] namely the GDPR and national systems governing electronic monitoring within work environments. To offer just one example, it is unclear if the classification of some AI systems as 'high-risk' results in the automatic triggering of the GDPR provisions that address high-risk processing. In other words, does the AI Act's classification reinforce the need to perform the impact assessment required by the GDPR with regard to AI systems used in relation to recruitment, selection, evaluation, monitoring, and decision-making based on personal data? And what about the antinomy between the GDPR's ban on solely automated decision-making and the unencumbered tolerance for the very same practice that informs the proposed PWD?

Given the unbalanced information and bargaining power between workers and employers, the introduction of new technologies that offer monitoring as well as data collection and processing capabilities is tightly regulated in the workplace. Workers and their representatives must be informed and consulted. In countries such as Germany, workers also wield co-determination powers. Article 88 of the GDPR allows Member States, 'by law or collective agreements', to introduce 'more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context'.[63] This provision aims at fostering responsive solutions to the emergence of new technologies and practices that may significantly affect workers' rights while also providing an opportunity to bring worker representatives (and, in some instances, data protection authorities [DPAs]) to the table for the purpose of involvement or co-determination.[64] Similarly, Article 20 of the PWD allows Member States to apply or introduce more favourable regulations for workers. The 'horizontal regulatory approach' adopted by the AI Act seems to underestimate these work-related exceptions.

The drafters of the AI Act are well aware of the potential clash between supranational and domestic regulations. Indeed, it has been clarified that the fact that 'an AI system is classified as high risk under [the AI Act] should not be interpreted as indicating that the use of the system is necessarily lawful under other acts of Union law or under national law compatible with Union

62. Artur Bogucki, Alex Engler, Clément Perarnaud, and Andrea Renda, 'The AI Act and Emerging EU Digital Acquis: Overlaps, Gaps and Inconsistencies' (Ceps In-Depth Analysis, 2022). See also Aída Ponce Del Castillo and Diego Naranjo, 'Regulating Algorithmic Management: An Assessment of the EC's Draft Directive on Improving Working Conditions in Platform Work' (ETUI Research Paper-Policy Brief, 2022) 8.

63. Halefom H Abraha, 'A Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace' (2022) 12(4) International Data Privacy Law 276. The GDPR refers 'in particular' to 'the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work', as well as 'the protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship'.

64. National data protection authorities state that compliance with domestic provisions concerning employee monitoring must be considered a precondition for meeting the requirements of the principle of lawful processing (GDPR Art. 5).

law, such as on the protection of personal data […]' (Recital 31).[65] Despite this laudable attempt to position the proposed AI Act within a more complex and varied web of rules, little has been said about the way in which such cross-reference can be concretely operationalised. The same is true for the scope of this caveat. The protection of personal data is indicated to be only an example of the EU and national laws that could be superseded by the AI Act. What are the other areas in which potential mismatches between the AI Act and other pieces of EU law or national law compatible with EU law could arise? Assigning the task of creatively interpreting this Recital to the national authorities is hazardous.[66]

Both the legal basis of the AI Act (Article 114 of the Treaty on the Functioning of the European Union [TFEU]) and its entire conceptualisation lean towards liberalising the production and marketing of AI systems in the EU, provided such systems comply with the standards set out in the Act. As discussed extensively elsewhere,[67] these standards are inadequate when it comes to curbing algorithmic management systems, which are increasingly common in today's world of work, as they completely neglect the role of the workers' representatives and trade unions in regulating the introduction of technological tools at work. Therefore, the liberalisation thrust - and the legal basis - underpinning this initiative risk surmounting any domestic regulations, including work-related ones, that mandate higher standards of protection.[68] As a result, fear exists that the AI Act would act as a 'ceiling' rather than a 'floor' of protection, an outcome that would not be unprecedented in the field of EU employment and labour legislation. Similar situations have notoriously occurred with regard to other legal provisions with a 'liberalising' aim, which were interpreted by the Court of Justice of the EU in the 'Laval Quartet' in such a way as to trump (fundamental) collective labour rights.[69]

Hence, more protective laws, including those established at the national level under Article 88 of the GDPR or Article 20 of the PWD, risk being watered down or quashed altogether if read as incompatible with the maximum harmonisation aims of the Regulation. The AI Act could be invoked before the Court of Justice of the EU in an effort to unsettle national frameworks providing for the involvement of the social partners prior to the introduction of any technological tool able to monitor workers' performance. This is particularly relevant when AI applications are embedded within ordinary tools already used in the workplace to protect business assets, assess work performance, or flag deviant behaviours (e.g., the mundane productivity tracking tools offered by collaborative software). While most ordinary monitoring devices, such as closed-circuit television, typically have to pass at least an information and consultation phase prior to being introduced in professional environments—and are sometimes also subject to administrative authorisation—the

65. 'Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law. This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant' (AI Act Recital 41).
66. Tadas Klimas and Jurate Vaiciukaite, 'The Law of Recitals in European Community Legislation' (2008) 15 ILSA Journal of International & Comparative Law 61.
67. Valerio De Stefano and Mathias Wouters, 'AI and Digital Tools in Workplace Management Evaluation: An Assessment of the EU's Legal Framework' (2022) European Parliamentary Research Services, Scientific Foresight Unit (PE 729.516).
68. Antonio Aloisi and Elena Gramano, 'Artificial Intelligence is Watching You at Work: Digital Surveillance, Employee Monitoring and Regulatory Issues in the EU Context' (2019) 41(1) Comparative Labor Law & Policy Journal 95.
69. Rotem Medzini, 'Governing the Shadow of Hierarchy: Enhanced Self-regulation in European Data Protection Codes and Certifications' (2021) 10(3) Internet Policy Review 1.

model envisaged by the AI Act could displace all such procedural protections. These due-process-like safeguards could, in fact, be interpreted as exorbitant and disproportionate relative to the rules provided by the AI Act and, therefore, be viewed as hampering the free provision of the AI-related services that the instrument aims to promote in accordance with the EU's market liberalisation goals.

An evident laissez-faire approach prevails within the draft AI Act.[70] The providers of AI systems merely have to comply with a 'set of horizontal mandatory requirements for trustworthy AI' listed in Chapter 2 of the Draft.[71] A 'practically unachievable' precondition[72] is the use of 'sufficiently' high-quality datasets in which the training, validation and testing are relevant, representative, free from error, and complete. The requirements also include:

- the establishment, implementation, and documentation of a risk management system (Article 9);
- 'appropriate data governance and management practices' in relation to training, validation, and testing datasets (Article 10);
- package-insert-like documentation proving compliance with current rules prior to commercialisation or entry into service (Article 11);
- automatic recording of certain crucial information (Article 12);
- transparency and 'interpretability' of procedures (Article 13);
- human oversight by natural persons so as to minimise risks to health, safety, and fundamental rights (Article 14); and
- 'an appropriate level of accuracy, robustness, and cybersecurity' (Article 15).

In practice, however, the requirements are mainly based on certification via the *ex-ante* 'conformity assessment procedures' conducted by the providers themselves or, in a limited number of cases (e.g., remote biometric identification), by external standard-setting bodies.[73]

When compared with the GDPR schemes, the AI Act's model is both overinclusive and toothless, at least when it comes to AI systems used for human resource management purposes. While shrouded in an illusion of simplicity and cost-effectiveness,[74] it is overinclusive due to the number of specific duties required to fulfil its techno-determinist goals, preventing those individuals affected from having a meaningful voice. One unintended consequence of the massive list of compliance requirements could be an excess of uncertainty, coupled with both high compliance costs for businesses and almost impossible enforcement for workers, trade unions, DPAs, and labour administrations. This could stifle innovation to the advantage of the big players.

70. Sümeyye Elif Biber, 'Machines Learning the Rule of Law: EU Proposes the World's First Artificial Intelligence Act' (*VerfBlog*, 13 July 2021) <https://verfassungsblog.de/ai-rol/> accessed 10 April 2023.
71. For the source of inspiration, see European Commission High-Level Expert Group on Artificial Intelligence, 'Sectoral Considerations on Policy and Investment Recommendations for Trustworthy AI' (2019).
72. Nathalie Smuha and Anna Morandini, 'Trustworthy AI through Regulation? Sketching the European Approach' (*The Digital Constitutionalist*) <digi-con.org/4-trustworthy-ai-through-regulation-sketching-the-european-approach/> accessed 28 November 2022.
73. Heiko Gerlach, 'Self-reporting, investigation, and evidentiary standards' (2013) 56 The Journal of Law & Economics 1061.
74. Gellert (n 16).

This model is also much less robust than that described in the (technology-agnostic) Article 22 of the GDPR, which bans solely automated decision-making with legally impactful consequences.[75] Although this prohibition is undermined by a significant carve-out (i.e., it does not apply when this type of processing is deemed 'necessary for entering into, or performance of, a contract between the data subject and a data controller', which could well be the case in relation to employment-related applications of automated decisions), section 3 requires the employer to 'implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests', which is coupled with a non-exhaustive list of safeguards such as the right to obtain human intervention, to express a point of view and to contest a decision.[76] A purposive interpretation of Article 22 would militate in favour of the existence of the right 'to obtain an explanation of the decision'.[77] Nothing analogous can be found within the AI Act.

Ensuring fairness, transparency, and accountability in terms of algorithmic management in the context of platform work is among the three specific objectives contributing to the overarching goal of the proposed PWD,[78] namely the improvement of the working conditions and social rights of people who work through digital labour platforms. For the first time, automated monitoring and decision-making are identified as possible sources of jeopardy for platform workers, due to contributing to both the precariousness of their working conditions and the diminished quality of their engagement.[79] If read in conjunction with the GDPR and the proposed AI Act, the PWD could lead to an unexpected situation in which persons performing platform work would, at least on paper, be protected to a much greater extent than 'ordinary' workers and data subjects (both employed and self-employed ones). At this stage, it is difficult to foresee whether the 'more focused' scope of the proposed PWD would steer it away from the deregulatory impact of the AI Act. It must be stressed, however, that both texts are still under discussion, now entering the final stages of the legislative procedure.

Chapter III of the proposed PWD introduces protection in relation to key managerial prerogatives executed through technological tools and software. Moreover, Article 6 mandates that platform workers be informed about the existence and specific scope of '(a) automated monitoring

75. Lee A Bygrave, 'Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision-Making' in Karen Yeung and Martin Lodge (eds), *Algorithmic Regulation* (Oxford University Press 2019). See also Antoni Roig Batalla, 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)' (2017) 8(3) European Journal of Law and Technology 1.
76. Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 235. According to GDPR Art. 35(9), controllers 'shall seek the views of data subjects or their representatives on the intended processing'.
77. GDPR Recital 71. For an overview, see Bryan Casey, Ashkan Farhangi, and Roland Vogl, 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34 Berkeley Technology Law Journal 145; Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-making and "a Right to Explanation"' (2017) 38 AI Magazine 55; Emre Bayamlıoğlu, 'The Right to Contest Automated Decisions under the General Data Protection Regulation: Beyond the So-called "Right to Explanation"' (2021) 16 Regulation & Governance 1058. See also Article 29 Working Party (n 39) 25.
78. The other two specific objectives are (i) the correct employment status classification and access to the applicable labour and social protection rights and (ii) transparency, traceability, awareness, and improved enforcement of the applicable rules. See Explanatory Memorandum (n 22) 3. See also Antonio Aloisi and Nastazja Potocka-Sionek, 'De-gigging the Labour Market? An Analysis of the "Algorithmic Management" Provisions in the Proposed Platform Work Directive' (2022) 15(1) Italian Labour Law e-Journal 29.
79. European Commission, 'Protecting People Working through Platforms: Commission Launches a First-stage Consultation of the Social Partners' (24 February 2021) 5 <https://bit.ly/3May6N3> accessed 10 April 2023.

systems which are used to monitor, supervise or evaluate the work performance of platform workers through electronic means' and '(b) automated decision-making systems which are used to take or support decisions that significantly affect those platform workers' working conditions'.[80] With regard to the systems included in (b), platform workers must be informed about the criteria used to make a decision, the 'weight' of each criterion, and 'the grounds for decisions to restrict, suspend or terminate the platform worker's account, to refuse the remuneration for work, on the platform worker's contractual status' and 'any decision with similar effects'.

Under Article 8, platform workers have the right to receive a written explanation of how such decisions were reached. This provision covers 'any decision *taken* or *supported* by an automated decision-making system that significantly affects the platform worker's working conditions' (emphasis added). The reference to the ancillary role of algorithmic tools gives the provision a broader scope than Article 22 of the GDPR (which is limited to decisions *solely* based on automated processing).[81] While the GDPR mandates 'suitable measures to safeguard the data subject's rights and freedoms and legitimate interests', the PWD requires a human review of significant decisions upon request by an affected person who has the right to contest a platform's practices. In addition, platforms must provide a written statement concerning semi- or fully automated decisions that have critical effects in areas such as the restriction, suspension or termination of accounts, denial of remuneration for work done, and contractual status. Moreover, workers can request the revision of a decision if the provided explanation does not prove persuasive or they feel hindered in relation to their rights. The platform is obligated to provide a detailed reply within a reasonable timeframe, 'without undue delay and in any event within one week of receipt of the request' (Article 8(2)).

The PWD also introduces robust information and consultation duties vis-à-vis workers' representatives regarding the introduction and alteration of automated monitoring and decision-making systems under Article 9—that is, a model that dwarfs any algorithmic impact assessment. However, the provision cannot be read as a full expression of the right to 'negotiate the algorithm',[82] nor does it cover genuinely self-employed workers, who are left to fend for themselves.[83] We have strongly decried the fact that automated monitoring and decision-making are seen as inherent to the platform business model, a view that subscribes to the common rhetoric of its natural 'inevitability'. Nonetheless, the PWD allows collective actors to learn about algorithmic systems before they are implemented and offer inputs concerning the adoption and revision of such systems. It has been demonstrated that the collective dimension is precisely where the social harms precipitated by algorithms reveal their strongest impacts.[84] In this respect, the existence of 'individualised' and 'remedial' data rights represents a blunt instrument because it does not prevent abuses from

80. Article 6 also bans some of the most abusive forms of data processing, including in relation to 'any personal data on the emotional or psychological state' of platform workers, data concerning their health, and private conversations. It also prohibits the collection of 'any personal data while the platform worker is not offering or performing platform work'.
81. Article 29 Working Party (n 39) 21. See also Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-making and Profiling' (2018) 34 Computer Law & Security Review 398.
82. Valerio De Stefano, '"Negotiating the Algorithm": Automation, Artificial Intelligence and Labour Protection' (2020) 41(1) Comparative Labor Law and Policy Journal 1.
83. De Stefano (n 41).
84. Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor, Bart van der Sloot, and Luciano Floridi (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017).

occurring, nor does it actually empower workers who lack the technological savvy, means and assistance necessary to engage in processes aimed at rebalancing information asymmetries.[85]

3.2 United States: pressure not to lag behind and preliminary steps

There is a great deal of buzz regarding the percolation of EU regulatory instruments into other jurisdictions due to their extraterritorial effects. This phenomenon is referred to as the 'Brussels effect', which reflects the capability of 'first mover' EU institutions to exercise power or influence over (the rest of) the world by means of legal norms, standards, and sanctions.[86] Although this soft authority concerns the 'spontaneous' compliance of companies interested in avoiding the costs associated with multiple regimes and standards, in the United States several acts and bills partially emulate the contents or, at least, the purposes of EU tools such as the GDPR. One key reason for this trend towards homologation is the desire on the part of certain policymakers not to be left behind by EU institutional activism in terms of the governance of technologies and 'digital constitutionalism' (i.e., the embedding of indefectible principles and values within the digital domain).[87] The EU acts as a 'regulatory entrepreneur' due to its commitment to conceptualising and operationalising a 'European approach' that combines the ability to reap the benefits of technological innovation with the need to safeguard fundamental rights and values.[88] However, the concrete results of this ambitious programme are mixed and do not translate the aspiration for a stronger social dimension into practice, as documented in the preceding section.

Recent developments are bringing the United States 'closer' to the EU in terms of the guardrails for AI tools.[89] The most prominent examples of this regulatory cross-fertilisation are the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), two 'prototypes' that may soon be replicated in other states. The CCPA (which came into effect in 2020) gives consumers more control over the personal data that companies collect about them. The previous 'employee-employer exemption' expired at the end of 2022. As a landmark law, it secures new-generation privacy rights for Californian consumers and workers, including (i) the right to know about the personal information a business collects about them and how it is used, sold, and shared; (ii) the right to delete personal information collected from them (with some exceptions); (iii) the right to opt out of the sale of their personal information; and (iv) the right to allege discrimination in relation to the exercise of their CCPA rights.

Approved in 2020 and entered into force in 2023, the CPRA represents one of the first attempts to secure privacy and data rights in the United States. It aims to reinforce the provisions of the CCPA. It must be noted that the CPRA significantly expands worker privacy rights by providing

85. But see Platform Work Directive art 9(2) on assistance by an expert to the benefit of platform workers' representatives.
86. Anu Bradford, 'The Brussels Effect' (2012) 107 Northwestern University Law Review 1. See also Giovanni Buttarelli, 'The EU GDPR as a Clarion Call for a New Global Digital Standard' (2016) 6(2) International Data Privacy Law 77.
87. Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorization' (2019) 33 International Review of Law, Computers & Technology 76.
88. Kristina Irion, Mira Burri, Ans Kolk, and Stefania Milan, 'Governing "European Values" inside Data Flows: Interdisciplinary Perspectives' (2021) 10(3) Internet Policy Review 1.
89. Veena Dubal, presentation at the Transatlantic Expert Group on the Future of Work, September 2022; Alex Engler, 'The EU and US Are Starting to Align on AI Regulation' (*Brookings*, 1 February 2022) <https://www.brookings.edu/blog/techtank/2022/02/01/the-eu-and-u-s-are-starting-to-align-on-ai-regulation/> accessed 10 April 2023. See also Stefania Palma et al, 'New US-EU Co-operation on Competition Policy Raises Boardroom Alarms' *Financial Times* (London, 21 December 2021) <https://on.ft.com/3CAbUch> accessed 10 April 2023.

notice duties, provisions on the correction of inaccurate 'personal information' and limits to the use and divulgation of sensitive personal data. Many commentators have drawn a parallel between this legal instrument and the GDPR.[90]

In the wake of these important developments (which have together led to the newly dubbed 'California effect'),[91] other states have adopted similar models, including the Colorado Data Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Protection Act. There are also some narrower instruments, such as the Illinois Artificial Intelligence Video Interview Act, which has been imposing disclosure, transparency, and erasure duties onto employers that use AI systems to analyse interviews for recruitment purposes since January 2020. Similarly, since October 2020 in Maryland, a new law prohibits employers from using facial recognition technology during pre-employment job interviews without first obtaining the candidate's consent.[92] Employers must inform applicants that AI is being used and disclose how the system works and which variables are under scrutiny. In addition, New York City's law 1894-A requires all AI-powered hiring tools to be audited for bias.[93] While this law does not enshrine actionable individual rights, it compels employers to disclose the adoption of any AI instruments used to automate recruitment procedures and conduct annual audits on them, with the results needing to be made publicly available.[94]

In California, Assembly Bill 701 (AB 701) entered into force in January 2022. It is designed to regulate the use of quotas within logistics warehouses. Certain large companies in the industry are required to disclose allocations and pace-of-work standards to each employee upon hiring. Moreover, a 'written description of each quota to which the employee is subject to, including the quantified number of tasks to be performed or materials to be produced or handled, within a defined period, and any potential adverse employment action that may result from failure to meet the quota' must be shared. Employees can disregard any quotas that prevent compliance with meal or rest periods, the use of bathroom facilities, or health and safety laws.[95] Another important development in this regard is the California Workplace Technology Accountability Act (AB 1651).[96] This proposed Act would confer on workers the right to be informed of, review, correct, and secure data collected from them by the employer. It would also enshrine the principles of data minimisation and purpose limitation, thereby limiting the ability of employers to use data beyond the indicated purposes. The impact of these provisions is compounded by the introduction of limitations on the

90. The CCPA defines 'personal information' as information that identifies, relates to, describes, is reasonably capable of being associated, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
91. Natasha Singer, 'Charting the "California Effect" on Tech Regulation' *New York Times* (New York, 12 October 2022) <https://www.nytimes.com/2022/10/12/us/california-tech-regulation.html> accessed 10 April 2023.
92. Angelica Salvi del Pero, Peter Wyckoff, and Ann Vourc'h, (2022), 'Using Artificial Intelligence in the Workplace: What Are the Main Ethical Risks?' (2022) OECD Social, Employment and Migration Working Paper No 273.
93. Local Law Int No 1894-A; see J Edward Moreno, 'New York City AI Bias Law Charts New Territory for Employers' (*Bloomberg Law*, 29 August 2022) <https://news.bloomberglaw.com/daily-labor-report/new-york-city-ai-bias-law-charts-new-territory-for-employers> accessed 10 April 2023.
94. Nicol Turner Lee and Samantha Lai, 'Why New York City is cracking down on AI in hiring' (*Brookings*, 20 December 2021) <https://www.brookings.edu/blog/techtank/2021/12/20/why-new-york-city-is-cracking-down-onai-in-hiring/> accessed 10 April 2023.
95. Shannon Bettis Nakabayashi and Ashley N Rippolone, 'California Passes Legislation Regarding Job Performance Quotas for Large Warehouse Facilities' (2021) XII(332) The National Law Review <https://www.natlawreview.com/article/california-passes-legislation-regarding-job-performance-quotas-large-warehouse> accessed 10 April 2023.
96. Airlie Hilliard, Emre Kazim, Tom Kemp, and Kelvin Bageire, 'Overview and Commentary of the California Workplace Technology Accountability Act' (2022) 37(1) International Review of Law, Computers & Technology 91.

collection and use of data obtained through electronic monitoring as well as certain redlines concerning the purposes and effects of automated decision-making. Significantly, the Act also requires employers that adopt hiring or management technologies to draft and publish a related impact assessment document.

Relatedly, the state of New York has advanced a more targeted Warehouse Worker Protection Act, which is known as the 'Amazon Warehouse Act'. Its key purpose is to make 'productivity quotas' more transparent within warehouses—that is, workers (and regulators) must be provided with documentation concerning their quotas and notified about any shift in the company's expectations with regard to the pace of work and deliverables. The Act bans the use of excessively stringent quotas that prevent workers from taking breaks for personal reasons. While this focus on quotas is suited to the perception of this instrument as regulating algorithms at work, its overarching purpose is actually to ensure compliance with health and safety regulations. Several news reports have exposed the harsh model whereby workers are reprimanded or even fired for their 'time off-task' (i.e., the time they spend on activities other than their legally required 30-minute lunch break). This pressure has also been identified as a source of the higher-than-normal injury and illness rates among Amazon workers.[97] Workers must receive information about their quotas within the first month of being hired and have the right to access both current and previous productivity data (up to a maximum of three months). Additionally, they are empowered to pursue a court injunction against any detrimental practices, whereas an excessively high injury rate triggers the possibility of a state investigation.

In October 2022, the White House Office of Science and Technology Policy published the Blueprint for an AI Bill of Rights. Despite its resonant title, the proposed AI Bill of Rights is a white paper, meaning that the included rights are not legally enforceable and are mostly addressed to the Federal Government. The outcome of an input-gathering process involving stakeholders and human rights advocates, the key principles of the Bill are the right to scrutiny over how data is used, the right to opt out of automated decision-making, the right to live free from ineffective or unsafe algorithms, the right to be informed of the fact that AI is making a decision about them, and the right to not be discriminated against by algorithms. Practically concomitantly, General Counsel Jennifer Abruzzo published a memo on behalf of the National Labor Relations Board (NLRB)[98] proclaiming the intention to focus on the electronic monitoring of workers which results in chilling effects on the organising and exercising of collective bargaining rights.[99] The document stresses the importance of enforcement to the agency's lawyers, who prosecute unfair labour practice cases, and the need to adopt a new framework 'to adapt the [NLRA] to changing patterns of industrial life'.[100] Significantly,

97. Strategic Organizing Center (SOC), 'Primed for Pain: Amazon's Epidemic of Workplace Injuries' (SOC, May 2021) <https://thesoc.org/wp-content/uploads/2021/02/PrimedForPain.pdf> accessed 10 April 2023; SOC, 'The Worst Mile: Production Pressure and the Injury Crisis in Amazon's Delivery System' (SOC, May 2022) <https://thesoc.org/wp-content/uploads/2022/06/The-Worst-Mile.pdf> accessed 10 April 2023.
98. The NLRB is an independent federal agency established in 1935 to protect employees from unfair labour practices and ensure the right of private sector employees to join together, with or without a union, to improve wages, benefits and working conditions.
99. Section 7 of the National Labor Relations Act (NLRA) on employees' ability to engage in protected activity. See Office of Public Affairs, 'NLRB General Counsel Issues Memo on Unlawful Electronic Surveillance and Automated Management Practices' (*National Labor Relations Board*, 31 October 2022) <https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and> accessed 10 April 2023.
100. *NLRB v J Weingarten, Inc* (1975) 420 US 251, 266.

given their extensive pervasiveness both at work and in private lives, algorithmic management tools and surveillance technologies are identified as systems that potentially impair collective rights.

3.3 Canada: the right to be informed (and not much more)

As mentioned above, in 2022, the Canadian Federal Government tabled Bill C-27, which includes legislation concerning consumer privacy protection (the CPPA) and AI and data (the AIDA). The most striking feature of this 'package' concerns the provisions regarding employment included within the CPPA. The proposed Act would apply 'to every organization in respect of personal information that…is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business'. Moreover, section 23 provides that 'an organization may collect, use or disclose an individual's personal information *without their knowledge or consent if it was produced by the individual in the course of their employment*, business or profession and the collection, use or disclosure is consistent with the purposes for which the information was produced' (emphasis added). In addition, section 24 allows organisations to 'use or disclose an individual's personal information' without their consent if 'the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the organization and the individual', provided that 'the organization has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes'.

Consequently, in federally regulated work (which includes, among others, the banking, mail, and radio and television broadcasting sectors), employers would have unfettered authority to introduce and use electronic and algorithmic management and monitoring systems, with individual employees having no recourse if they were informed about the existence and use of such systems. In unionised workplaces, employers would arguably still be required to negotiate the introduction of such systems under sections 51–55 of the Canada Labour Code. The lack of any substantial protection in all other circumstances is, however, extremely concerning. At the provincial level, the only significant legislation in this regard is Ontario's Working for Workers Act of 2022. Its approach is not dissimilar to that of the CPPA. It mandates that businesses with more than 25 employees adopt a written policy outlining whether they monitor employees electronically, in what fashion and for what purposes, albeit without attaching any substantial protection to these procedural provisions.[101]

4. Towards 'participatory AI governance'?

Our analysis has elucidated the intricacies of the current piecemeal legislation regulating AI systems for automated decision-making in work environments. We have underlined the weaknesses of the existing instruments and presented the perils associated with the risk-based approach. This jigsaw of provisions has two opposite poles: the PWD and the AI Act. The proposed PWD fleshes out credible safeguards for platform workers who are exposed to algorithmic management. Yet, the related set of provisions do not extend beyond the boundaries of platform work, prompting scholars, commentators, and Members of the European Parliament[102] to call for a more

101. Moreover, in Ontario, no statutory provisions analogous to Sections 51–55 of the Canada Labour Code are in place.
102. European Parliament Committee on Employment and Social Affairs, 'Report on the proposal for a directive of the European Parliament and of the Council on improving working conditions in platform work' COM (2021) 0414(COD) <https://www.europarl.europa.eu/doceo/document/A-9-2022-0301_EN.html> accessed 10 April 2023.

'universalistic' approach,[103] as such practices pose enormous challenges to national and EU labour protection systems. The PWD could serve as an 'experiment'[104] able to 'pave the way for a broader approach to the use of [AI] in the labour market in the near future'.[105] This shows the genuine ambition of the EU Commission and markedly contrasts with the AI Act's potentially liberalising effects, which represent a significant threat to the working conditions and labour rights of 'logged-in' workers. In light of this, it seems all the more urgent to address the tension between the protections enshrined within Chapter III of the proposed PWD and the minimalist intervention of the AI Act.

Given the purposes,[106] limited scope, and specific legal bases of the PWD, coupled with the option for Member States to design a more strongly protective framework that is enshrined in Article 20, it is safe to suggest that the proposed PWD should be read as a *lex specialis* to both the 'horizontal' AI Act and, to a certain extent at least, the GDPR. Alternative interpretations are plausible, although they would have implicitly abrogative effects on the provisions of the PWD, something that would seem counterintuitive to the purposes of instruments adopted by the same legislative bodies during the same period.[107] However, this unsolved conflict brings us back to the untenable choice to limit the scope of application of the provisions regulating algorithmic decision-making (at the individual and collective levels) laid down within Chapter III of the PWD to only platform workers. While it is not clear whether genuine self-employed platform workers will be included within the final version of the text, leaving outside the scope of its protection all workers who are not engaged by platforms reduces the impact of these promising provisions, thereby furthering the segmentation of data protection schemes.

In addition, in conjunction with Article 88 of the GDPR, the PWD expressly allows the introduction and application of more vigorous levels of protection by Member States. This provision should, therefore, be used to 're-empower' at the EU level initiatives such as the Spanish *Ley Rider*, which sets out collective transparency rights with regard to the logic, metrics, and parameters computed by AI tools adopted by companies in all industries and sectors.[108] It could also be used to

103. Aislinn Kelly-Lyth and Jeremias Adams-Prassl, 'The EU's Proposed Platform Work Directive: A Promising Step' (*VerfBlog*, 14 December 2021) <https://verfassungsblog.de/work-directive/> accessed 10 April 2023.

104. We do not use this definition in a technical manner, as Chapter III does not meet the key requirements of a regulatory experiment in terms of the temporal scope, indication of the goals, and transparency of and adherence to legality principles. For a general discussion, see Ranchordás (n 53). See also Jon Truby, Rafael Dean Brown, Imad Antoine Ibrahim, and Oriol Caudevilla Parellada, 'A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications' (2022) 13 European Journal of Risk Regulation 270.

105. European Commission, 'Analytical Document accompanying the consultation document Second-phase consultation of social partners under Article 154 TFEU on possible action addressing the challenges related to working conditions in platform work' SWD(2021) 143 final, 24.

106. The difficulties associated with being classified as employees (or 'workers') leave the people who perform platform work more vulnerable to algorithmic domination, opacity, and abuses. The vast majority of transparency and information rights are mainly reserved for 'workers', including those featured within Directive (EU) 2019/1152 of the European Parliament and of the Council of 20 June 2019 on transparent and predictable working conditions in the European Union. Pursuant to Platform Work Directive Art. 1(2), this Directive applies to 'every worker in the Union who has an employment contract or employment relationship as defined by the law, collective agreements or practice in force in each Member State with consideration to the case-law of the Court of Justice'. For an analysis of the personal scope of the DTPWC, see Despoina Georgiou, 'The New EU Directive on Transparent and Predictable Working Conditions in the Context of New Forms of Employment' (2022) 28 European Journal of Industrial Relations 193.

107. De Stefano (n 41).

108. Ane Aranguiz, 'Spain's Platform Workers Win Algorithm Transparency' (Social Europe, 18 March 2021) <https://socialeurope.eu/spains-platform-workers-win-algorithm-transparency> accessed 10 April 2023.

strengthen the German Co-Determination Act concerning algorithmic management as well as the national provisions concerning technological surveillance that have long existed in some Member States. The very narrow scope of the proposed PWD leaves us wondering if the choice to introduce ambitious information and consultation rights of platform workers' representatives (Article 9) in a 'sectoral' instrument was appropriate. Several reasons have been advanced in the preparatory documents in support of such a move, although the prominence and recrudescence of algorithmic decision-making well beyond the context of the gig economy render the PWD an idiosyncratic model that is easy to circumvent and difficult to enforce given the 'compliance entrepreneurship' applied by platforms.[109]

The AI Act has shortcomings that need to be addressed. In chasing the mirage of harmonisation, the proposed Regulation may end up lowering the bar of protection, despite purporting to fight abuses with an extra layer of procedural burdens whose enforcement is left to the regulatees, whose role may be reduced to 'rubber-stamping'. To overcome the 'who-controls-the-controllers' dilemma triggered by the pre-emptive conformity assessment that the providers of high-risk AI systems must conduct, a possible solution would be shifting the burden of proof onto the providers of AI used for employment purposes. They should be able to demonstrate the 'innocuousness' and 'non-toxicity' of such systems before placing them on the market by involving the workers affected by AI systems and their representatives.[110] Otherwise, such systems would be considered 'unlawful by default'.[111] Moreover, AI-enabled managerial tools pose a number of risks to workers' rights well beyond the realm of privacy. Thus, full consistency must be ensured with the EU Charter of Fundamental Rights and the secondary EU legislation concerning consumer protection, equality and non-discrimination, and health and safety. To foster legal certainty, the introduction of an explicit provision preventing any national labour and employment regulation from being 'dismembered' under the AI regulation would be useful.

Another pitfall to be avoided is the 'individualised' understanding of the related rights and principles,[112] an issue that also concerns the PWD due to its exclusion of persons who perform platform work outside the framework of employment relationships from the collective aspects of the rights to information and consultation with regard to automated decision-making systems. The proposed PWD singles out Article 16(2) of the TFEU as the legal basis for its AI-related provisions, which allows for the adoption of rules 'relating to the protection of *individuals* with regard to the processing of personal data' in order to secure informational self-determination. This wording does not seem to presuppose any distinction based on contractual statuses. A growing body of literature is questioning the atomistic mobilisation of data rights.[113] This shortcoming is exacerbated by the prevalence of risk-based approaches that typically iron out individual differences and allow any profiles that deviate from the 'average man' to suffer 'the consequences of

109. Elizbeth Pollman and Jordan M Barry, 'Regulatory Entrepreneurship' (2016) 90 Southern California Law Review 383.
110. For an analogy with Article 5 of Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH), see Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law 19.
111. Gianclaudio Malgieri and Frank A Pasquale, 'From Transparency to Justification: Toward Ex Ante Accountability for AI' (2022) Brooklyn Law School Legal Studies Paper No 712.
112. Jay Youngdahl, 'Solidarity First: Labor Rights Are Not the Same as Human Rights' (2009) 18 New Labor Forum 30.
113. Salome Viljoen, 'Democratic Data: A Relational Theory for Data Governance' (2021) 13 Yale Law Journal 573; Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 475.

a policy that treats them as invisible and their needs of little worth'.[114] Here, algorithms and AI tools operate at the level of groups, communities, and populations, particularly in professional contexts.[115] Thus, collective rights represent a way forward, even though practical hurdles such as decreased unionisation rates, scarce collective bargaining coverage, and lack of digital literacy could render them weaker.

The emerging consensus among experts is that the labour-related category included in the list of high-risk AI systems should be entirely scrapped from the AI Act.[116] In a similar vein, the narrow provisions concerning algorithmic management that cover platform workers leave a great deal to be desired in terms of their scope of application. The now-pervasive role of AI constitutes a challenge in almost all socio-economic areas and, therefore, requires interventions capable of overcoming the logic of watertight regulatory silos. Professional relationships are always unbalanced when it comes to bargaining power and information asymmetries. This condition is exacerbated by opaque data-driven tools when they are used without collective scrutiny. Hence, it will be vital to ensure that the EU social *acquis* is enforced and strengthened in the legislative instruments that are currently under discussion.[117] At the same time, it would be short-sighted to assume that the existing frameworks are sufficient. While the organisational structures and strategies facilitated by AI tools are certainly not novel, their scale, scope and volume are genuinely unprecedented. A more fruitful way to make fundamental rights work would be the adoption of a dedicated EU instrument regulating technology in workplaces and providing a non-waivable level of protection.

Until recently, the introduction of productivity-enhancing technological systems in work contexts was focused on business assets owned by the employer, such as machinery and goods, which sometimes resulted in significant indirect effects on workers (e.g., the introduction of assembly lines impacted both tasks and pace). These changes were often considered part of employers' managerial prerogatives and, therefore, protected under the freedom to conduct business, even if, in certain jurisdictions, co-determination and information and consultation rights 'tempered' the unilateral exercise of such prerogatives. It is questionable, however, if the same conceptual apparatus and legal framework centred on the freedom to conduct business can be borrowed for technologies whose primary object is workers' physical body and intellectual conduct, as in the case of AI-enabled surveillance and management systems. These systems target people, not goods or assets. This suggests that the primary thrust of any regulation of such systems should be centred on the protection of fundamental rights, not on economic freedoms and techno-deterministic assumptions whereby anything technically possible should be allowed.

The impacts of AI and (labour) algorithms on the nature, organisation, and quality of work are rarely advantageous.[118] Several successes have been achieved thanks to strategic litigation, with

114. Kaminski (n 52).

115. A stronger collective dimension can be found within the GDPR. Trade union representatives can file a claim before a court or exercise a data protection right before the employer or the DPA 'independently of a data subject's mandate' (GDPR Art. 80). Clara Krämer and Sandrine Cazes, 'Shaping the Transition: Artificial Intelligence and Social Dialogue' (2022) OECD Social, Employment and Migration Working Paper No 279.

116. Jeremias Adams-Prassl, Halefom Abraha, Aislinn Kelly-Lyth, Michael 'Six' Silberman, and Sangh Rakshita 'Regulating Algorithmic Management: A Blueprint' (elsewhere in this issue).

117. Kullmann and Cefaliello (n 30).

118. Abigail Gilbert and Anna Thomas, *The Amazonian Era: How Algorithmic Systems are Eroding Good Work* (Institute for the Future of Work, 2021) 29. European Agency for Safety and Health at Work, *Artificial Intelligence for Worker Management: An Overview* (EU-OSHA, 2022) 20–23.

trade unions having mobilised data protection, transparency and non-discrimination rights and acted as collective claimants before national DPAs and labour courts.[119] Nevertheless, such achievements cannot compensate for the imbalance between informational and bargaining powers, as they are issued on a case-by-case basis and often only bind those parties to the relevant legal action. Thus, concrete advancements in the field are slow to materialise, which makes the case for both targeted new regulations and the recalibration of existing rules more urgent.[120] In searching for a better solution to a pressing problem than new instruments such as the AI Act or the North American instruments, and in line with the pledge made by the General Counsel for the NLRB, we conclude with a call to advance 'participatory AI governance', namely bottom-up approaches that promote multi-stakeholder involvement in order to ensure that due process and fundamental rights are respected in the work context.

In light of the high stakes involved, the promotion of compliance cannot be left solely to the developers and adopters of such technologies. Even assuming that all 'conformity boxes' are ticked[121] and, therefore, that AI tools receive a 'compliance green light', power gaps remain wide open because the extent of managerial prerogatives is inordinately intensified when such tools are adopted in workplaces. Given the limitations of current regulatory frameworks and the uncertainty brought about by partially overlapping models, and while enforcing current regulations remains a crucial priority for authorities, it is time to envision a comprehensive supranational instrument that regulates the use of technologies that perform monitoring, decisional, and disciplinary functions in professional ecosystems. A meaningful shift towards human-centric models requires collective codetermination and, importantly, co-design of AI- and algorithm-based systems throughout their entire life cycle, whereby representative bodies are involved to ensure that innovations are deployed in such a way as to not impinge on fundamental labour rights.

Acknowledgements

We are grateful to the convenors and participants of the 'Regulating Algorithmic Management' workshop, which was held at Magdalen College, Oxford, in July 2022. We are also thankful to Rocco Iodice, Nastazja Potocka-Sionek, and Antonella Zarra for their generous comments on an earlier draft of this article.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

Antonio Aloisi's contribution to this article is made within the framework of the 'Boss Ex Machina' project, which has received funding from the European Union's Horizon 2020 research and innovation programme under Marie Skłodowska-Curie grant agreement No 893888. Valerio De Stefano's contribution is supported by the Canada Research Chair programme.

119. Sebastião Barros Vale and Gabriela Zanfir-Fortuna, 'Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities' (Future of Privacy Forum, 2022).
120. Adams-Prassl et al (n 116).
121. Karen Yeung, Andrew Howes, and Ganna Pogrebna, 'AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing' in Markus D Dubber and Frank Pasquale (eds), *The Oxford Handbook of AI Ethics* (Oxford University Press, 2020).