Check for updates

Special Issue Contribution

ELLJ

European Labour Law Journal
2023, Vol. 14(2) 172–191
© The Author(s) 2023

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20319525231167317
journals.sagepub.com/home/ell

Regulating algorithmic employment decisions through data protection law

Halefom Abraha
Postdoctoral Researcher, Bonavero Institute of Human Rights, University of Oxford, Oxford, UK

Abstract
The regulation of algorithmic management falls under the purview of multiple legal domains including but not limited to labour law, non-discrimination law and data protection law. While labour law does not have explicit provisions to adequately protect workers from algorithmic harms, existing non-discrimination and data protection laws can address some aspects of these harms. This article examines the extent to which the GDPR offers the necessary tools to protect workers from harm stemming from algorithmic management. It argues that while the provisions tailored to automated decision-making (ADM) and the rest of the GDPR provide workers with some limited protections, significant gaps remain. It then suggests some policy options on how the existing protections under the GDPR can be further complemented, particularised, and strengthened through a combination of legislative and non-legislative measures.

Keywords
Algorithmic management, GDPR, privacy, data protection, labour law, workers' data rights

1. Introduction

Algorithmic management[1] tools proliferate everywhere across industries. First introduced in digital labour platforms, algorithmic management systems are now increasingly used across the socio-economic spectrum, in conventional employment settings, and by all categories of companies (small, medium, and large). One industry study claimed that '99% of Fortune 500 companies'

1. This article uses the expression 'algorithmic management' and 'automated decision-making' interchangeably for the sake of convenience.

Corresponding author:
Halefom Abraha, Postdoctoral Researcher, Bonavero Institute of Human Rights, University of Oxford, Oxford, UK.
Email: halefom.abraha@law.ox.ac.uk

rely on algorithmic decision-making tools.[2] A Harvard Business School study also found that even midsize enterprises (of between 50 and 999 employees) use algorithmic management systems 'quite extensively.'[3] These findings demonstrate that algorithmic management 'is likely to become a prominent feature in many people's jobs in the next few years.'[4]

Algorithmic management systems can be used at different stages of the employment lifecycle. At the recruitment stage, algorithmic management systems could be used to target job advertisements, screen and rank applications, decide which applicants to invite to interviews, and evaluate candidates during interviews by analysing different aspects of communication such as facial expressions, body language, word choice, and tone of voice.[5] During employment relationships, these tools could be used for allocating and directing of work, controlling and monitoring of workers, evaluating workers' performance, predicting workers' future behaviour, and disciplining or firing workers.[6]

Complex algorithmic management tools are increasingly used to make high-stakes decisions that have traditionally been made by human managers, and these tools could significantly change working conditions and social relationships and pose significant risks to the dignity, health, equal treatment, and autonomy of workers. It is extensively documented that algorithmic management systems may perpetuate historical patterns of discrimination and pose significant challenges to workers' data protection and privacy rights. As highlighted at the outset of this Special Issue, the increasing deployment of algorithmic management tools in the workplace has further intensified the informational and power asymmetries in the employment relationship. The fact that workers do not understand how algorithmic management systems function means that they cannot effectively

2. James Hu, '99% of Fortune 500 Companies Use Applicant Tracking Systems' (*Jobscan*, 7 November 2019) <https://www.jobscan.co/blog/99-percent-fortune-500-ats/> accessed 1 October 2022; Eric Reicin, 'AI Can Be A Force For Good In Recruiting And Hiring New Employees' (*Forbes*, 16 November 2021) <https://www.forbes.com/sites/forbesnonprofitcouncil/2021/11/16/ai-can-be-a-force-for-good-in-recruiting-and-hiring-new-employees/> accessed 30 September 2022.
3. Joseph B. Fuller and others, 'Hidden Workers, Untapped Talent: How Leaders Can Improve Hiring Practices to Uncover Missed Talent Pools, Close Skills Gaps, and Improve Diversity' (Harvard Business School 2021) <https://www.hbs.edu/managing-the-future-of-work/research/Pages/hidden-workers-untapped-talent.aspx> accessed 30 September 2022; Chris Vallance, 'AI Tools Fail to Reduce Recruitment Bias: Study' (*BBC News*, 13 October 2022) <https://www.bbc.com/news/technology-63228466> accessed 18 November 2022.
4. Valerio De Stefano, 'AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU's Legal Framework' (European Parliamentary Research Service, PE 729516 2022).
5. Jérémie Giniaux-Kats and others, 'Taking Back Control of AI at Work: 20 Proposals to Promote Responsible Algorithmic Management' (Leplusimportant, in partnership with Geneva Macro Labs 2021); Jenny Yang, 'Ensuring a Future That Advances Equity in Algorithmic Employment Decisions' (2020) Testimony before the House Education and Labor Committee, United States House of Representatives <https://www.urban.org/research/publication/ensuring-future-advances-equity-algorithmic-employment-decisions> accessed 30 September 2022; Danielle Ochs, Jennifer G Betts and Zachary V Zagger, 'California's Draft Regulations Spotlight Artificial Intelligence Tools' Potential to Lead to Discrimination Claims' (*Ogletree Deakins*, 13 May 2022) <https://ogletree.com/insights/californias-draft-regulations-spotlight-artificial-intelligence-tools-potential-to-lead-to-discrimination-claims/> accessed 9 October 2022.
6. Giniaux-Kats and others (n 5); Spencer Soper, 'Fired by Bot at Amazon: "It's You Against the Machine"' (*Bloomberg.com*, 28 June 2021) <https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out> accessed 7 October 2022; Cheryl Teh, '"Every Smile You Fake": An AI Emotion-Recognition System Can Assess How "Happy" China's Workers Are in the Office' (*Business Insider Nederland*, 16 June 2021) <https://www.businessinsider.nl/every-smile-you-fake-an-ai-emotion-recognition-system-can-assess-how-happy-chinas-workers-are-in-the-office/> accessed 9 October 2022.

bargain over their data rights and, hence, the balance of power continues to tilt towards the employer.

The ubiquitous deployment of algorithmic management systems in the workplace means that these systems 'act as modern gatekeepers to economic opportunity.'[7] Consequently, efforts to scrutinise the use of these systems are on the rise across the globe. Experts agree that it is time to regulate algorithmic management, and policymakers are starting to take note. In Europe, existing and proposed laws including the General Data Protection Regulation (GDPR), the proposed Artificial Intelligence (AI) Act and the proposed Platform Work Directive recognise that algorithmic management tools carry high risks to employees. The AI Act, for instance, identifies two aspects of algorithmic management—recruitment and workplace management—as 'high risk.'[8] Inspired by several court rulings and data protection authority (DPA) decisions, the proposed Platform Work Directive also details algorithmic transparency requirements, as shall be discussed later.

The emerging policy proposals in the EU and elsewhere show that there is a growing consensus that existing regulatory tools are not enough and that algorithmic management systems need specific regulatory treatment. However, it must also be noted that some of the risks of algorithmic management can be met by existing regulations. While the regulation of algorithmic management falls under the purview of multiple legal domains including labour law and non-discrimination law, data protection law has been the area of law that is most engaged, owing to the vast troves of personal data processing underpinning the majority of these tools.[9] It is for this reason that some of the most pressing issues raised in the AI regulation discourse are directly related to the fundamental principles of data protection, such as fairness, transparency, and accountability. For instance, in its comprehensive analysis of AI policies across the world, the Center for AI and Digital Policy found that 'AI policy safeguards follow from other laws and policy frameworks, most notably data protection.'[10] Although it is not yet sufficiently explored, data protection law—specifically the GDPR—has already been used to challenge some of the intensive and novel algorithmic management practices, particularly in the context of platform work.[11]

This raises a crucial question: what regulatory tools does the GDPR offer to tackle the risks that algorithmic management systems pose to the fundamental rights and freedoms of workers? This article examines the potential and limits of the GDPR in regulating algorithmic management systems. It considers the adequacy of the provisions of the GDPR specifically tailored to automated decision-making and the limitations of data protection law as a regulatory instrument more broadly.

The discussion proceeds in four parts. The next section examines in detail the key regulatory tools of the GDPR in the context of algorithmic management. It discusses legal and practical challenges encountered when trying to use GDPR to regulate algorithmic management. Section 3 considers the overlap between data protection and labour laws. This section shows that some of the

7. Yang (n 5).
8. 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) recital 36 and Annex III.
9. Giovanni Sartor, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (European Parliamentary Research Service 2020).
10. 'Artificial Intelligence and Democratic Values Index' (Center for AI and Digital Policy 2022) 3 <https://caidp.org/reports/aidv-2021/> accessed 9 October 2022.
11. For a comprehensive analysis of court rulings and DPA decisions on automated decision-making under the GDPR, see 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).

issues that arise in the context of algorithmic management do not neatly fit within the remit of data protection law. Section 4 offers some possible ways forward, identifying legislative and non-legislative policy actions for different stakeholders. The last section concludes.

2. Key regulatory tools of the GDPR relevant to algorithmic management

The GDPR applies in its entirety to algorithmic management if personal data processing is involved.[12] This section thus focuses only on data rights and safeguards that are particularly tailored to algorithmic management systems. The GDPR recognises that automated decision-making entails a high risk to workers and provides additional and strict transparency and accountability requirements.

2.1. The right to be informed

One of the underlying policy objectives of the GDPR is to give data subjects—here, workers—control over their personal data. This objective cannot be realised unless workers are aware that their personal data is being processed by employers, and have access to that data. Workers must be made aware of risks, rules, safeguards, and rights in relation to algorithmic management and how to exercise these rights in relation to such processing.[13] The right to be informed constitutes the prerequisite to counterbalance the informational and power asymmetry in the employment relationship and to invoke other data rights, including rectification, deletion, and data portability.

Articles 12–14 of the GDPR provide *ex-ante* obligations on what, how, and when workers must be informed in relation to the processing of their personal data.[14] Also referred to as the information obligation,[15] this transparency requirement has three salient components.[16] The first component is the content of the information. This aspect addresses the categories and sources of information that must be provided to the worker.[17] This requirement applies regardless of whether personal data are collected from the worker or from other sources. The latter source of personal data is particularly relevant in the employment context, as employers often collect job applicants' personal data from different sources, including social media, former employers, recruitment agencies, and other databases.[18] Another important aspect of the information obligation is that it is not limited to personal

12. For details on how the rest of the GDPR applies to fully automated and semi-automated decisions, regardless of Article 22 conditions, see ibid 13–18.
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) recital 39.
14. These obligations are applicable without being invoked by the worker.
15. GDPR recital 60.
16. For details on this, see EDPB, 'Guidelines 01/2022 on Data Subject Rights: Right of Access' (adopted 18 January 2022; Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (WP259 rev 01, revised and adopted on 11 April 2018).
17. Articles 13–14 of the GDPR provide an extensive list of information that must be provided to the employee.
18. For instance, the online publication of non-anonymised employment tribunal judgments making it easier for employers to search the names of job applicants against those listed as claimants. For details on this, see Zoe Adams, Abi Adams-Prassl and Jeremias Adams-Prassl, 'Online Tribunal Judgments and the Limits of Open Justice' (2021) 41 Legal Studies 1.

data processing, but also includes information on processing operations and information on workers' rights.

The second aspect of the notification obligation concerns the time frame for the provision of information. The GDPR provides different requirements depending on the source of personal data and the purpose of processing. Where the data are collected directly from the worker, the information must be provided at the earliest stage of the processing life cycle, i.e., 'at the time when personal data are obtained.'[19] The GDPR provides a different time requirement when the data are collected from other sources, in which case information must be provided 'within a reasonable period after obtaining the personal data, but at the latest within one month.'[20] In the case of 'further processing' for a purpose other than that for which the personal data were obtained, the employer should provide workers with the required information prior to that further processing.[21]

The modality by which information must be provided to the worker constitutes the third component of the notification obligation. The GDPR requires information to be provided to the worker 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language.'[22] What these requirements would mean in practice depends on the circumstances of the data processing.[23] Although the GDPR does not prescribe a particular modality, employers are required to 'take appropriate measures' that fit the circumstances of their data processing practices. These components of the information obligation (content, timing, and modality) also apply to the right of access (discussed below).

The mere provision of information in relation to the processing of personal data neither meets the requirements of fairness and transparency within the meaning of the GDPR nor puts workers in a position to exercise their rights effectively. The GDPR recognises this shortcoming and requires employers to inform workers of the existence of data rights and facilitate the exercise of these rights, specifically the data rights provided under Articles 15–22. Most importantly, the GDPR recognises that fully automated decision-making entails high risks and imposes additional and strict transparency and accountability requirements. The employer must inform workers about the existence of automated decision-making and provide meaningful information about the logic involved, as well as the significance and the envisaged consequences. The corresponding rights of this notification obligation are further explained as follows.

2.2. The right of access

Similar to the right to be informed, the right of access enables workers to have control over their data.[24] Without the right of access, workers would not be in a position to exercise other data rights effectively. While the GPDR provides extensive information and access rights (including confirmation of whether personal data are processed, access to the data, and information about

19. GDPR Art. 13(1).
20. ibid Art. 14(3)(a).
21. ibid Arts. (13)(3), (14)(4).
22. ibid Art. 12.
23. Article 29 Working Party, 'Guidelines on transparency' (n 16) para 24.
24. EDPB (n 16) para 5; see also Bart Custers and Anne-Sophie Heijne, 'The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in Theory and Practice' (2022) 46 Computer Law & Security Review 105727 (noting that 'the right of access is about control and empowerment of data subjects').

the processing itself), Article 15(1)(h) exclusively applies to the context of automated decision-making, providing workers with the right to know how algorithmic management is used. As per this provision, workers have:

(a) the right to be informed of the existence of automated decision-making, including profiling;
(b) the right to obtain meaningful information about the logic involved; and
(c) the right to be informed of the significance and the envisaged consequences of such processing for the data subject.

In contrast to the *ex-ante* information obligation discussed above, which requires information to be provided within a specified time and in the appropriate modality, Article 15 provides an *ex post* right of access that applies only when invoked by the worker. Workers can invoke these rights at any reasonable interval. Workers can leverage the right of access to counterbalance information asymmetry in algorithmic management, exercise other rights, and voice their concerns. Furthermore, the right of access can serve as 'organizing and power-building tools' for workers.[25] For instance, some trade unions and civil society organisations have recently supported Amazon warehouse workers from multiple countries (Germany, the UK, Italy, Poland, and Slovakia) to file data access requests under Article 15.[26] However, the right of access in the context of automated decision-making as currently framed under Article 15(1)(h) of the GDPR has several shortcomings, three of which are worth noting.

2.2.1. Lack of clarity

The first ambiguity relates to the extent of information about algorithmic management that employers are required to give workers. Although the mere provision of information about the existence of solely automated decision-making is straightforward, the remaining requirements (meaningful information about the logic involved and the significance and the envisaged consequence) remain controversial and lead to uncertainties in practice.[27] In the face of complex algorithmic management systems deployed in the workplace, what type of information meets the criterion of 'meaningful information' within the meaning of Article 15(1)(h)? Can the requirement of 'meaningful information about the logic involved' be interpreted to include the right to explanation of a specific algorithmic decision?

The GDPR does not define what constitutes 'meaningful information about the logic involved', but existing literature suggests that it should be interpreted in line with the underlying aim of the right of access, and the principle of transparency.[28] Recital 63 shows that the objective of the right of access is to enable data subjects to 'be aware of, and verify, the lawfulness of the processing.' Further specifying this objective, the European Data Protection Board (EDPB) has stated that

25. Jake Stein and Dan Calacci, 'Workers Collective Data Access Rights: Adding Context to Worker Data Protection' (2022 preprint) <https://www.dcalacci.net/papers/202.10.10-collective-data-access-latest.pdf>.
26. 'Under the GDPR, Amazon Workers Demand Data Transparency' (*UNI Global Union*, 14 March 2022) <https://uniglobalunion.org/news/gdpr_amazon/> accessed 22 September 2022.
27. Custers and Heijne (n 24).
28. ibid; Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233.

'the purpose of the right of access is to make it possible for the data subject to understand how their personal data are being processed as well as the consequences of such processing.'[29] The principle of transparency also requires that 'any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.'[30]

Therefore, the information provided to workers about algorithmic management can be considered meaningful if it helps workers understand how their personal data are being processed, examine and verify the lawfulness of the processing, and enable them to exercise their rights. In other words, information that is too generic or too detailed may not contribute to achieving these objectives and thus fail to meet the criterion of meaningfulness. For instance, a technical and complex description of the algorithmic management system or merely mentioning that an automated decision-making system is being used cannot be considered meaningful. Similarly, the EDPB has stated that meaningful information about the logic involved does not necessarily include a complex explanation of the algorithms used or disclosure of the full algorithm.[31] Instead, the EDPB has noted, 'the information provided should (..) be sufficiently comprehensive for the data subject to understand the reasons for the decision.'[32] This interpretation takes us to the question of whether the right of access should include access to the algorithmic management system (software) itself. As Bart Custers and Anne-Sophie Heijne aptly point out, access to the automated decision-making system itself 'may not contribute to empowerment and control of the data subject, as most data subjects will be unable to read and understand the code.'[33]

2.2.2. Qualifications and limitations

The right of access is also subject to qualifications and limitations. First, employers can refuse or limit the right of access if this is necessary to protect the rights and freedoms of others.[34] Second, employers may use the intellectual property exception (Recital 63) to limit or refuse the right of access by workers.[35] Custers and Heijne have recently noted that 'it is unsurprising that companies may be very reluctant to share [information covered by IP rights] with data subjects, fearful that such disclosures may end up in the hands of competitors.'[36] The protection of trade secrets typically covers the AI system developed or purchased by the employer, but could perhaps also cover inferred data.[37] Data produced by workers as part of their work could also be subject to trade secret protection unless the data are used in ways that affect workers, such as for evaluating workers' performance.[38]

29. EDPB (n 16) para 10.
30. GDPR recital 39.
31. Article 29 Working Party, 'Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679' (last revised and adopted on 6 February 2018) 25.
32. ibid.
33. Custers and Heijne (n 24) 6.
34. GDPR Art. 15(4).
35. This exception may not, however, be used as an excuse to refuse access to all data. ibid Recital 63.
36. Custers and Heijne (n 24).
37. ibid.
38. Sara Baiocco and others, 'The Algorithmic Management of Work and Its Implications in Different Contexts' (JRC Working Papers Series on Labour, Education and Technology 2022/02); Stein and Calacci (n 25).

The protection against excessive requests is the third limitation. Article 12(5) allows employers to reject data access requests that are manifestly excessive. Furthermore, Recital 63 indicates that employers can ask workers to specify the data they wish to receive or the processing activities about which they wish to be informed. This requirement could significantly affect the right of access in the context of algorithmic management. For instance, in the case involving ride-hailing drivers and Uber, the latter invoked Recital 63 of the GDPR and asked the applicants for a specification of the personal data that applicants wish to receive because it processes a large amount of data. The district court of Amsterdam agreed with Uber, rejecting the right of access request for being too general and not sufficiently specified.[39] The requirement of specification assumes that workers know all the categories of personal data collected by their employers, which is not usually the case in practice. Research shows that workers often lack a clear understanding of the extent of the data collected, and of the technical functioning of the processing.[40] If workers do not know the personal data and the processing activities, asking them for specifications would run counter to the objective of the right of access.

2.2.3. Narrow scope

Not all automated decision-making processes automatically trigger the application of Article 15(1)(h). The GDPR makes a distinction between the transparency obligations that are applicable to fully automated decisions and the transparency obligations applicable to automated decisions that do not fall under Article 22. For workers to invoke the right of access in algorithmic management, the decision must be solely automated and produce legal effects or similarly significant effects within the definition of Article 22(1). If an algorithmic decision is made with human involvement, or a fully automated decision does not have a legal or significant effect, the algorithmic transparency requirement under Article 15(1)(h) does not apply.

It is not entirely clear why these rights should be restricted only to fully automated decisions with significant effect. This lack of clarity leads to conflicting interpretations by courts and DPAs. For instance, the EDPB recommends that it is a good practice (not mandatory) to provide the right of access under Article 15(1)(h), even if the decision is not fully automated.[41] Some DPAs follow a different approach: the Austrian DPA, for instance, is consistent in its stance that the specific transparency obligations under Article 15(1)(h) are not limited to solely automated decisions, but encompass other automated decisions even if they do not meet the high threshold established by Article 22.[42] The District Court of Amsterdam in the *Uber* case also followed a similar approach, extending the transparency provisions of Articles 13 and 14 and requiring the disclosure of the 'meaningful information about the logic involved' even though the algorithmic decision did not

39. *Rechtbank Amsterdam*, Case C/13/687315 HARK 20-207, ECLI:NL:RBAMS:2021:1020 (March 11, 2021) para 4.35 <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020> accessed 9 October 2022.
40. Eurofound, 'Employee Monitoring and Surveillance: The Challenges of Digitalisation' (Publications Office of the European Union, Luxembourg, 2020) 7.
41. Article 29 Working Party, 'Guidelines on Automated Individual Decision-making and Profiling' (n 31) 25.
42. *Austria Data Protection Authority*, ECLI:AT:DSB:2020:2020.0.436.002 <https://www.ris.bka.gv.at/Ergebnis.wxe?Suchworte=ECLI%3AAT%3ADSB%3A2020%3A2020.0.436.002&x=0&y=0&Abfrage=Gesamtabfrage> accessed 09 October 2022.

meet the Article 22 criteria.[43] This interpretation is arguably prudent for at least two reasons: First, most automated decisions today have human involvement, which makes the right of access to 'meaningful information about the logic involved' all the more important.[44] Second, 'small or insignificant (decisions) when considered alone, can add up to substantial collective impact when taken together.'[45]

2.3. Specific protection against algorithmic management

Article 22 of the GDPR constitutes the single most important safeguard against harms posed by algorithmic management. This provision recognises that humans, not algorithms, should make high-risk decisions, prohibiting solely automated decision-making with significant effects, such as whether someone deserves a job.[46] However, Article 22 also remains the most complex and controversial provision, in both theory and practice. This complexity prompted the UK government to consider a radical change—scrapping Article 22 GDPR altogether—although the idea was later dropped after strong opposition from stakeholders.[47]

The provision is not only vaguely drafted but also is subject to multiple layers of carve-outs that significantly weaken the practical efficacy of the specific safeguards. For instance, the prohibition on solely automated decisions is subject to a series of exceptions.[48] A solely automated decision which significantly affects workers is justified if the decision is (i) necessary for entering into, or performance of, a contract; (ii) authorised by Union or Member State law; or (iii) based on explicit consent. The contractual necessity exception is particularly relevant for the purpose of this article as employers usually rely on this legal basis to deploy algorithmic management systems. For instance, if an employer processes a vast amount of data from thousands of job applicants, the employer could use the 'contractual necessity' exception to justify a fully automated candidate screening process.[49]

43. *Rechtbank Amsterdam* (n 39). See also Barros Vale and Zanfir-Fortuna (n 11) 22.
44. Ben Green and Amba Kak, 'The False Comfort of Human Oversight as an Antidote to A.I. Harm' (*Slate* 15 June 2021) <https://slate.com/technology/2021/06/human-oversight-artificial-intelligence-laws.html> accessed 28 September 2022 (arguing that 'the binary of solely automated decisions versus those made by humans obscures the reality that most A.I. systems lie on some continuum between the two').
45. Robin Allen and Dee Masters, 'Technology Managing People—The Legal Implications' (Trades Union Congress 2021) 89.
46. The ambiguity of this provision has sparked a scholarly debate on whether Article 22(1) is a right to be actively invoked by the data subject or an outright prohibition. Although it is poorly drafted and its wording suggests otherwise, many scholars and data protection authorities see Article 22(1) as a prohibition. See, for instance, Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76; Luca Tosoni, 'The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation' (2021) 11 International Data Privacy Law 145.
47. 'Data: A New Direction' (Department for Digital, Culture, Media and Sport 2021) <https://www.gov.uk/government/consultations/data-a-new-direction> accessed 7 July 2022. Instead, the government plans to amend the provision to clarify the circumstances in which it must apply. See 'Data: A New Direction—Government Response to Consultation' (*Gov.uk*, updated 23 June 2022) <https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation> accessed 9 July 2022.
48. For an excellent analysis on this, see Pual De Hert and Guillermo Lazcoz, 'Radical Rewriting of Article 22 GDPR on Machine Decisions in the AI Era' (*European Law Blog*, 13 October 2021) <https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/> accessed 28 September 2022.
49. Article 29 Working Party, 'Guidelines on Automated Individual Decision-making and Profiling' (n 31) 23.

The contractual necessity, explicit consent, and Union or Member State law exceptions are themselves subject to another exception under Article 22(4): the exceptions to solely automated decision-making do not apply when the decisions are based on special categories of personal data referred to in Article 9(1) GDPR. Although at first glance this would seem to ban fully automated decision-making based on sensitive data, the protection is watered down by yet another exception: solely automated decisions based on special categories of data can be justified by explicit consent or reasons of substantial public interest based on Union or Member State laws.

If the employer relies on the contractual necessity or explicit consent exception to justify fully automated decisions with significant effects on workers, the employer is required to implement specific safeguards under Article 22(3). In these situations, workers have:

(a) the right to obtain human intervention;
(b) the right to express one's point of view;
(c) the right to contest the decision; and
(d) the right to obtain an explanation of the decision reached.[50]

While important, it is not well established how these procedural safeguards, particularly the right to human intervention and the right to explanation, apply in practice. As Jenny Yang noted, 'the complexity and opacity of many algorithmic systems often make it difficult if not impossible to understand the reason a selection decision was made.'[51] Compounding this complexity, most of the algorithmic management tools used in the workplace are developed, provided, and controlled by third parties (not by employers themselves), leaving employers with little understanding of, or control over, the systems.[52]

Similar complexities and uncertainties exist concerning the right to obtain human intervention. According to the EDPB, the requirement 'based solely on automated processing' under Article 22(1) does not necessarily mean that there is no human involvement in the decision at all. It rather means that a decision is made without any prior and meaningful assessment by a human.[53] This then gives rise to a series of other questions: what constitutes meaningful human involvement? How do we ensure that the requirement of human oversight does not lead to a box-ticking exercise? At which stage of the decision-making process is human involvement required?

These questions do not have an explicit answer in the GDPR. However, a systematic analysis of automated decision-making (ADM) jurisprudence across the EU reveals that courts and DPAs assess 'the entire organizational environment where an ADM is taking place…in order to decide whether a decision was "solely" automated or had meaningful human involvement.'[54] Although inconsistencies still exist, such assessments include the organisation structure, reporting lines, effective training of staff, and whether the decision is validated by different

50. GDPR Art. 22(3), read together with Recital 71.
51. Yang (n 5).
52. For instance, reports show that over one-third of the Fortune 100 companies use the same automated candidate screening AI. See 'Want a Job? The AI Will See You Now' (*MIT Technology Review*, 7 July 2021) <https://www.technologyreview.com/2021/07/07/1043089/podcast-want-a-job-the-ai-will-see-you-now-2/> accessed 24 October 2022.
53. Article 29 Working Party, 'Guidelines on Automated Individual Decision-making and Profiling' (n 31).
54. Barros Vale and Zanfir-Fortuna (n 11) 28.

people.[55] The application of such broad and multi-factor requirements could address the concern that employers can easily avoid meaningful human involvement in superficial ways or that humans could defer their decisions to algorithms by simply relying on algorithmic recommendations.[56]

Inconsistency also exists concerning the stage of the decision-making process where meaningful human involvement is required. For instance, the report by the Future of Privacy Forum found that courts and DPAs assess 'the last stage of the decision-making process' to determine whether there is meaningful human involvement or not.[57] This means that whether human involvement is meaningful or not depends on the extent to which the human influences the final decision, or whether it is the algorithm or a human being who has a final say on the outcome of the decision. However, conflicting interpretations abound as to what constitutes the last stage of a decision-making process. For instance, the EDPB is of the opinion the employer may invoke contractual necessity (Article 22(2)(a) of GDPR) to justify a fully automated candidate screening process if the processing involves a vast amount of data from thousands of job applicants.[58] By contrast, some national DPAs have ruled that fully automated shortlisting of job applicants can only be carried out with prior consent of the applicants under Article 22(2)(c) of GDPR.[59]

2.4. Algorithmic impact assessment

Long conceived as part of the accountability-based framework in data protection law, the impact assessment has become a central governance tool in AI regulation proposals globally. Although limited in scope, the GDPR provides a crucial starting point requiring an *ex ante* data protection impact assessment (DPIA) where processing is 'likely to result in high-risk to the individuals' rights and freedoms.'[60] It also sets out what a typical DPIA should contain (including a systematic description of the envisaged processing, an assessment of the necessity and proportionality, an assessment of the risks to the rights and freedoms of data subjects, and the measures envisaged to address the risks).[61] The GDPR does not define the high-risk threshold, but Article 35(3) provides a non-exhaustive list of such processing activities, which includes automated decision-making. The European guidelines on DPIA also classify employee monitoring as high-risk for meeting the criteria of (i) vulnerable data subjects (Recital 75), and systematic monitoring (Article 53).[62] Consistent with this guideline, at least 17 European DPAs have included

55. ibid.
56. Green and Kak (n 44); 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 (arguing that 'it would be easy to introduce a nominal human into the loop, "rubber stamping" automated decisions in order to knock out art 22 rights').
57. Barros Vale and Zanfir-Fortuna (n 11) 29.
58. Article 29 Working Party, 'Guidelines on Automated Individual Decision-making and Profiling' (n 31) 23.
59. Barros Vale and Zanfir-Fortuna (n 11) 9.
60. GDRP Art. 35.
61. GDPR Art. 35(7).
62. 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' (last revised and adopted 4 October 2017).

employment monitoring in their list of processing operations which are always subject to the requirement for a DPIA.[63]

The impact assessment regime under Article 35 GDPR has two key elements particularly relevant to algorithmic management: the need for workers' involvement, and prior consultation with DPAs. Theoretically, these requirements are crucial to identifying and addressing algorithmic harms. For instance, Article 35(9) GDPR requires employers to involve workers or their representatives in the process of DPIA. At first glance, this requirement seems to give workers a role to play, which is a crucial first step to collaborative algorithmic governance. Unfortunately, the practical application of the consultation requirement is severely restricted: workers or unions will be consulted for their views only where appropriate. This is limiting, as what is appropriate will be determined by the employer and hence the participation of workers or their representatives strongly depends on the willingness of the employer. The consultation process can also be further restricted for reasons of 'protection of commercial or public interests or the security of processing operations.' Furthermore, the fact that the GDPR does not require the publication of the results of the impact assessment, even to workers or their representatives, means that workers have no means to voice their concerns.

Under Article 36 GDPR, employers have the legal obligation to consult the national supervisory authority prior to processing, where a DPIA indicates that the processing would result in high risk and where the employer cannot sufficiently address these risks. If the employer fails to consult the relevant national authority, the latter can take enforcement actions, including imposing administrative fees or banning the processing altogether.[64] While this theoretically opens the opportunity for independent scrutiny of algorithmic management tools, there are several factors that could undermine its practical efficacy. For instance, the employer is obliged to seek prior consultation from the supervisory authority only when the former cannot find a sufficient measure to mitigate the risk. However, there are no common criteria for specifying when the supervisory authority shall be consulted. It is left for the employer to choose whether to consult the supervisory authority. This approach puts a lot of faith in the employer with no incentive to seek consultation. For instance, the practice in the UK shows that employers hardly approach the national supervisory authority for consultation, despite high-risk processes being carried out on a daily basis.[65] Compounding this lack of incentive for consultation is the absence of mandatory public disclosure of impact assessments.[66]

Lastly, even if the employer decides to consult the relevant national supervisory authority, the effectiveness of the scrutiny of risk mitigation strategies depends on the capacity of that supervisory authority.[67] As shall be discussed below, however, national supervisory authorities often lack resources, expertise, and priority to enforce the GDPR in the workplace, let alone effectively scrutinise complex algorithmic management systems.

63. For list of national DPIA guidelines, see 'EU Member State DPIA Whitelists, Blacklists and Guidance' <https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/> accessed 8 October 2022.
64. See GDPR Art. 58.
65. See 'Data: A New Direction' (*Gov.uk*, 10 September 2021 and updated 23 June 2022) paras 171–173 <https://www.gov.uk/government/consultations/data-a-new-direction> accessed 7 January 2022 (noting that 'prior consultation under Article 36 is infrequently used').
66. Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations' (2021) 11 International Data Privacy Law 125 (noting that the lack of mechanism for mandatory disclosure to the public is the biggest shortcoming of the DPIA regime under the GDPR).
67. Reuben Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 International Data Privacy Law 22; Kaminski and Malgieri (n 66).

3. The inadequacy of the GDPR in the field of labour

The preceding section highlighted the limitations of specific provisions of the GDPR relevant to algorithmic management. This section looks at some of the limitations of data protection law as a regulatory instrument more broadly, as algorithmic management has far-reaching implications beyond data protection, including consequences for work organisation and working conditions.

3.1. The problem of consent as a legal basis

One of the distinct features of personal data processing in the employment context is the nature of the employer-employee relationship, which is a relationship of power. Such a relationship of power challenges some of the key underlying principles of data protection law, such as consent. In order for consent to be acceptable as a legal basis, two conditions must be met: the data subject must (1) have adequate information and understand the processing; and (2) be able to consent freely. Neither of these is true in the employment context. The deployment of opaque and sophisticated algorithmic management tools further undermines the validity of consent. In the context of algorithmic management, data processing is often very complex, making it very difficult for workers to be informed about it.

For this reason, there is a widespread agreement among policymakers, data protection regulators and practitioners that 'employees are almost never in a position to freely give, refuse or revoke consent.'[80] Although regulators agree that employers should generally not normally rely on consent as a legal basis for employee data processing, in practice they still do. While Article 22(1) prohibits automated decision-making that significantly affects workers, employers can still circumvent this prohibition by relying on explicit consent under Article 22(2)(c) and Article 22(4) of the GDPR. These provisions suggest that consent is a suitable ground in the context of algorithmic management. For this reason, it can be argued that Article 22 GDPR does not provide adequate protection for workers. In its recent resolution calling for the creation of a new data protection legislation, the German Conference of the Federal and State Data Protection Authorities (DSK) reached the same conclusion, declaring that Article 22 of the GDPR provides insufficient protection for employees.[68] Policymakers seem to take note of this limitation. As shall be discussed below, the proposed Platform Work Directive takes a decisive step in the right direction by excluding consent as a legal ground to deploy algorithmic management systems.

3.2. The individualistic nature of data protection law

The GDPR has a problem with the way it conceives privacy harms; it is designed based on the categorical assumption that privacy harms are always individual and that these harms can be mitigated by giving individuals control over their personal data. These assumptions ignore that the idea of giving individuals control over their data is largely theoretical as technology becomes increasingly sophisticated. The GDPR also ignores collective and societal data protection and privacy harms, particularly the inherently collective nature of employment relationships. Therefore, the GDPR's exclusive focus on individual data subjects and individual rights does not easily fit with workers' rights and interests.

68. 'Resolution of the Conference of Independent Data Protection Authorities of the Federation and the Länder of 29 April 2022' <https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk> accessed 2 October 2022.

The information and power asymmetry in employment relations cannot be addressed only at the individual level. This is particularly true in the context of algorithmic management where an employee could be affected more by the data on other employees than by data collected on them.[69] These collective harms need a collective response.[70] As Martin Tisné has noted, 'protecting individual data is not enough when the harm is collective.'[71] There are extensive calls for establishing collective data rights for workers.[72] Although these calls have recently gained more traction among policymakers and practitioners, there is a long way to go in translating the emerging initiatives into practice. In this regard, the proposed Platform Work Directive takes a decisive step in the right direction by recognising collective data rights in algorithmic management.[73] The Spanish Riders' Law is another good case in point.[74]

3.3. Regulatory fragmentation

Workers' data protection in the EU is regulated by a patchwork of diverging legislative and non-legislative instruments across the 27 Member States, providing different degrees of protection. This fragmentation emanates from the GDPR itself. Through its various opening clauses, the GDPR allows diverging solutions to several issues, including data processing in the employment context. Two opening clauses of the GDPR are particularly relevant for the purpose of this article: Article 88 GDPR allows Member States to introduce more specific legal frameworks based on their respective national peculiarities and legal traditions. Utilising this broad opening clause, the Member States can, through legislation or collective bargaining agreements, regulate employers' personal data processing activities, covering the entire employment life cycle from recruitment to termination and everything in between.[75] The other relevant opening clause, Article 22(2)(b), authorises automated decision-making in derogation from the general prohibition under Member State law. Because of this opening clause, Member States have adopted diverging approaches to regulating automated decision-making; the result is diverging levels of protection in different Member States.[76] Interestingly, the list of specific safeguards under Article 22(3)—the right to obtain human intervention, the right to express one's opinion, the right to contest the

69. Martin Tisné, 'The Data Delusion: Protecting Individual Data Is Not Enough When the Harm Is Collective' (Stanford University's Cyber Policy Center 2022) <https://luminategroup.com/posts/report/the-data-delusion> accessed 2 October 2022.
70. Nathan Newman, 'Reengineering Workplace Bargaining: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace' 85 University of Cincinnati Law Review 68 (arguing that 'challenging information asymmetry in workplace requires collective rights and negotiation').
71. Tisné (n 69).
72. Christina Colclough, 'Towards Workers' Data Collectives' in Sohel Sarkar and Amay Korjan (eds), *A Digital New Deal: Visions of Justice in a Post-Covid World* (Just Net Coalition and IT for Change 2021) <https://projects.itforchange.net/digital-new-deal/2020/10/22/towards-workers-data-collectives/> accessed 2 October 2022; Adrian Todolí-Signes, 'Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection' (2019) 25 Transfer: European Review of Labour and Research; Stein and Calacci (n 25); Justin Nogarede, 'No Digitalisation without Representation: An Analysis of Policies to Empower Labour in the Digital Workplace' (FEPS Policy Study, November 2021).
73. 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) art 6(4).
74. Organic Law 3/2018 of December 5, Protection of Personal Data and Guarantee of Digital Rights art 64.
75. For a comprehensive analysis of Article 88, see Halefom H Abraha, 'A Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace' (2022) International Data Privacy Law ipac015.
76. For a comprehensive analysis of Article 22(2)(b) and the different approaches adopted by Member States, see Gianclaudio Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35 Computer Law & Security Review 105327.

decision, and the right to obtain an explanation—do not apply if the decision-making is authorised under Member State law. The GDPR only states that the applicable Member State law should lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. It does not explain what these suitable measures would constitute.

3.4. Enforcement challenges

The enforcement of data protection rules at work falls under the regulatory remits of DPAs, who are not labour experts. Multiple reports show that DPAs are under-resourced and understaffed.[77] Compounding the lack of resources and expertise is the lack of interest on the part of DPAs to prioritise data protection in the employment context.[78] A survey by the Future of Privacy Forum reveals that of the 12 European DPAs involved in their study, only three featured employment as a strategic and operational priority in their plan for 2020 and beyond.[79] Data protection in the workplace also escaped any mention in the EDPB's Work Programme 2021/2022.[80] Although workers' representatives are best placed to uphold data protection rules in the workplace and have the interest and legitimacy to do so, they also lack resources and technical expertise.[81] Furthermore, workers' representatives are uneven in their presence across the EU.[82]

Several experts, practitioners, and policymakers have suggested different options to address the enforcement challenges of data protection in the workplace, and specifically the regulatory challenges of algorithmic management. For instance, one of the extensively discussed solutions is to involve trade unions and workers' representatives in the decision-making process of how and under which conditions algorithmic management systems should be used in the workplace. This solution goes to the extent of 'making algorithmic management a topic of social dialogue in its own right.'[83] Although the primary role of these workers' representatives is negotiating labour-related issues such as employment standards, working conditions, and wage levels, they are increasingly assuming new data protection-related roles. Adopting a collaborative regulatory approach is another possible solution where DPAs and labour authorities share regulatory competencies to ensure proper oversight over the use of algorithmic management.[84] Such a collaborative regulation recognises that DPAs or labour authorities alone cannot ensure the effective implementation of algorithmic management rules in the workplace owing to the complexity

77. 'Is the GDPR Doing Its Job?' (*MLex*, 20 September 2022) <https://mlexmarketinsight.com/news-hub/special-reports/is-the-gdpr-doing-its-job>accessed 09 Oct 2022.
78. Nogarede (n 72) 17–18; De Stefano (n 4) 65.
79. Charlotte Kress, Rob Van Eijk, and Gabriela Zanfir-Fortuna, 'New Decade, New Priorities: A Summary of Twelve European Data Protection Authorities' Strategic and Operational Plans for 2020 and Beyond' (Future of Privacy Forum, 12 May 2020).
80. 'EDPB Work Programme 2021/2022' <https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf> accessed 8 October 2022. With thanks to Justin Nogarede for helping me realise this point.
81. Justin Nogarede, 'Workers Data Rights' (Employment Policy Breakfast Series, 13 September 2022) <https://feps-europe.eu/event/workers-data-rights/> accessed 14 November 2022.
82. ibid.
83. Giniaux-Kats and others (n 5) 51; Valerio De Stefano and Simon Taes, 'Algorithmic Management and Collective Bargaining' (ETUI Foresight Brief series 2021).
84. For more on collaborative regulation, see 'The Digital Regulation Cooperation Forum' (*Gov.uk*, 10 March 2021) <https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum> accessed 8 July 2022.

of the systems and the cross-cutting nature of the regulatory functions. The proposed Platform Work Directive envisages a collaborative regulatory approach by allocating competencies among DPAs and labour authorities and requiring them to exchange relevant information relating to their respective regulatory functions.[85] This approach should be further strengthened and expanded beyond platform work.

4. Some ways forward

The gaps in current legislation have given rise to calls for specific regulation in the workplace. Although these calls have been long-standing, they have become increasingly urgent with the increasing deployment of algorithmic management systems.[86] Some promising regulations have been adopted or proposed in response to these calls for establishing new data rights in the context of algorithmic management.[87]

This section suggests some policy options on how the existing protections under the GDPR can be further complemented, particularised, and strengthened through a combination of legislative and non-legislative measures.

4.1. Legislative action at the EU level

The first and preferable option is for the EU to step in and take legislative action, in particular, through a specific Directive addressing the risks of algorithmic management. This European response can be done either by introducing a new Directive[88] or by expanding the scope of the recently proposed Platform Work Directive. The Platform Work Directive represents a significant step forward, increasing and clarifying the transparency regime of the GDPR regarding automated monitoring and decision-making systems. It establishes several rights including, but not limited to, the right to be informed, the right to explanation, the right to review a decision, and the right to rectification. The proposed Directive has certain elements that make it stronger than the GDPR in regulating automated monitoring and decision-making systems. For instance, the proposed Directive:

- Expands the algorithmic transparency regime of the GDPR, to cover both solely automated and semi-automated decisions.[89]
- Establishes a collective right to information by requiring digital labour platforms to make algorithmic management systems intelligible to platform workers, their representatives and labour authorities.[90]
- Prohibits the processing of personal data 'not intrinsically connected to and strictly necessary for the performance of the contract' and bans the processing of any personal data 'on the emotional or psychological state' of platform workers under all circumstances.[91]

85. Platform Work Directive Art. 19.
86. For instance, Michael Schwemmle and Peter Wedde, 'Shift of Power in the Digital Work Environment—The German Case: Employees Need New Rights!' (*Friedrich-Ebert-Stiftung* 2019).
87. For instance, Platform Work Directive; Organic Law 3/2018 (n 74).
88. The 'Blueprint' in this *Special Issue* outlines what a legislative action at the EU level should look like.
89. Platform Work Directive Art. 6(1)(b).
90. ibid Art. 6(4).
91. ibid Art 6(5).

- Imposes system-level impact assessment requirements and establishes explicit rights to obtain an explanation and/or review of significant decisions in individual cases.[92]
- Excludes consent as a legal basis to justify algorithmic management.[93]

The significant shortcoming of the proposed Platform Work Directive is that its scope of application is limited to platform workers and persons performing platform work. This means that if the Directive is adopted in its current format, platform workers who have an employment relationship will have more protection than traditional employees. This approach risks creating 'an inconsistent regulatory environment that places workers in legal uncertainty.'[94] The European legislature can fix this inconsistency either by expanding the scope of the Directive to cover all workers subject to automated or semi-automated decisions, as recommended by the Committee on Employment and Social Affairs,[95] or by introducing a new and complementary legal instrument.

4.2. Legislative actions at the Member State level

Member States can also take the initiative to address the current gaps in regulating algorithmic management. Member States can avail themselves of the opportunity created under Article 88 of the GDPR and introduce independent employee data protection laws that meet the special requirements of processing personal data in the workplace and specifically address the risks of algorithmic management. Unfortunately, Article 88 is 'still massively underutilised.'[96] In this regard, there is a promising development in Germany with significant political momentum for developing new, free-standing workplace data protection legislation (also addressing the data protection aspects of algorithmic management), which could also open the opportunity for other Member States to follow suit.[97]

4.3. The need for collective agreements

Article 88 of the GDPR also lays the foundation for social partners to play an essential role in the governance of data protection, including algorithmic management in the workplace.[98] Should social partners properly utilise this opportunity, collective agreements could address the risks posed by algorithmic management. In fact, Valerio De Stefano argues that 'collective bargaining

92. ibid Art. 8. Addressing the concerns raised with regard to the GDPR, the proposed Directive requires an explanation of algorithmic decisions to be given by a person who has the necessary competence, training, and authority to exercise that function.
93. Platform Work Directive art 6(5).
94. 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 Policy Brief 2022).
95. European Parliament Committee on Employment and Social Affairs, *Draft Report on the proposal for a directive of the European Parliament and of the Council on improving working conditions in platform work* (2021/0414(COD)).
96. De Stefano (n 4) 41; see also Abraha (n 75); Nogarede (n 72).
97. For details on this, see Halefom Abraha, Michael 'Six' Silberman and Jeremias Adams-Prassl, 'The Need for Employee-Specific Data Protection Law: Potential Lessons from Germany for the EU' (*European Law Blog*, 30 September 2022) <https://europeanlawblog.eu/2022/09/30/the-need-for-employee-specific-data-protection-law-potential-lessons-from-germany-for-the-eu/> accessed 8 October 2022.
98. This provision explicitly provides that specific data protection measures in the employment context can be provided via collective agreements.

is the most effective tool to provide safeguards against the rapid technological developments in algorithmic management.'[99]

The Riders' Law in Spain represents a blueprint for this approach. The law is the result of a tripartite collective bargaining agreement reached between trade unions, employer organisations, and the Spanish Government. Although limited to the platform economy, the Riders' Law provides for arguably adequate data rights in algorithmic management, at both the individual and collective levels.[100] At the EU level, the European Framework Agreement on Digitalisation adopted in 2020 explicitly refers to Article 88 of the GDPR and the ways in which more specific rules on workers' data protection can be laid down via collective agreements.[101] The Agreement sets out some directions and principles of how and under which circumstances algorithmic management systems should be used in the workplace, including the principle of 'guaranteeing the human in control.'[102] While a commendable and positive step in the right direction, the Agreement fails to provide clear and binding guidance on how and under which circumstances algorithmic management systems should be used in the workplace.[103]

4.4. The need for new guidance

In the context of a rapidly changing world of work, an instrument to guide employer data practices is sorely needed—for workers and employers alike. Unfortunately, there is currently no clear guidance on how the provisions of the GDPR should be interpreted in the workplace, despite the repeated calls for such guidance.[104] The Article 29 Working Party's Opinion of 2/2017 on data processing at work is neither up to date (it is based on the 1995 Data Protection Directive) nor endorsed by the EDPB. The EDPB should step in and issue concrete guidance on personal data processing in the employment context, specifically on how and under which circumstances algorithmic management systems should be used in the workplace.

4.5. Codes of conduct and certification schemes

Voluntary codes of conduct and certification schemes could also offer, at least in the short term, the potential to mitigate some of the risks posed by algorithmic management. Both codes of conduct and

99. De Stefano and Taes (n 83) 8; Valerio De Stefano, '"Masters and Servers": Collective Labour Rights and Private Government in the Contemporary World of Work' (2020) 36 International Journal of Comparative Labour Law and Industrial Relations 425, 442.
100. Organic Law 3/2018 (n 74). Following the adoption of this law, the first collective agreement was signed in 2021 between the digital labour platform Just Eat and the Spanish trade union confederations CCOO and UGT. See also 'Collective Agreement Just Eat' (*Digital Platform Observatory*) <https://digitalplatformobservatory.org/initiative/collective-agreement-just-eat/> accessed 8 October 2022. The Ministry of Labour also launched a guide for companies to comply with the obligation to report on the use of algorithms at both the individual and collective levels. See 'The Ministry of Labour Publishes a Guide on the Use of Algorithms' (*Eurogip*, 1 August 2022) <https://eurogip.fr/en/spain-the-ministry-of-labour-publishes-a-guide-on-the-use-of-algorithms/> accessed 20 November 2022.
101. 'European Framework Agreement on Digitalisation' (BusinessEurope, SMEunited, CEEP and the ETUC 2020) 12.
102. ibid 11.
103. Nogarede (n 72) 32 (noting that 'the agreement does not provide binding interpretations of, for instance, the GDPR, nor clear guidance on how its provisions should be applied in the world of work').
104. Frank Hendrickx, Elena Gramano and David Mangan, 'Privacy, Data Protection and the Digitalisation of Work: How Industrial Relations Can Implement a New Pillar' (*Global Workplace Law & Policy*, 26 June 2020) <http://global-workplace-law-and-policy.kluwerlawonline.com/2020/06/26/privacy-data-protection-and-the-digitalisation-of-work-how-industrial-relations-can-implement-a-new-pillar/> accessed 8 October 2022; De Stefano (n 4); Nogarede (n 72).

certification constitute part of the accountability-based regulatory framework of the GDPR, whereby employers can demonstrate compliance with their data protection obligations. However, they remain the least-explored tools.

The introduction of codes of conduct and certification schemes as accountability tools is premised on two underlying assumptions. The first assumption is that specific sectors can have specific needs regarding the requirements of the GDPR.[105] On the other hand, 'organisations within the same industry, or engaging in similar types of processing, are likely to encounter similar data protection issues'[106] and this is where the merits of codes of conduct and certification schemes tailor-made to such similar data protection issues arise. The second and related assumption is that the GDPR is not particularised enough to encompass all the specific needs of each sector or processing operation. This is particularly true in the employment context, where personal data processing is distinct from other contexts in many aspects.

Trade unions or employers' associations can prepare codes of conduct.[107] These employment-specific associations have the incentives and expertise to identify the algorithmic risks that their members might encounter, assess the origin, nature, likelihood and severity of these risks, and articulate best practices to mitigate such risks.[108] Furthermore, employment-specific bodies are best placed to calibrate the data protection obligations for their respective members. Specifically, codes of conduct can particularise and clarify the application of the GDPR, such as regarding fair and transparent processing, the collection of personal data, and the extent of information to be provided to workers.[109]

5. Conclusion

The analysis above shows that applying existing law to algorithmic management is not sufficient. Particularly, the analysis demonstrates that the specific provisions of the GDPR regulating automated decision-making do not adequately address workers' data rights in algorithmic management. Although the GDPR requires, as a principle, that only a human being should make consequential decisions such as whether someone gets a job or gets fired, this prohibition can be circumvented by the exceptions such as contractual necessity and consent. Furthermore, most decisions today are algorithmically assisted, not fully automated, in which case none of the safeguards of Article 22(3), such as the right to contest the decision, apply. More broadly, the GDPR is not a sufficient regulatory tool to address all the harms that arise from algorithmic management. With the increasing deployment of algorithmic management systems across the socio-economic spectrum, it is high time for policymakers and relevant stakeholders to step in and take decisive measures in protecting workers from algorithmic harms. This can be achieved through legislative actions at Union and Member State level and non-legislative interventions such as through collective bargaining, specific guidance, and codes of conduct.

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.

105. This assumption is reflected under Regulation (EU) 2016/679 Protection of natural persons with regard to the processing of personal data and on the free movement of such data in Art. 40(1).
106. Detlev Gabel and Tim Hickman, 'Impact Assessments, DPOs and Codes of Conduct—Unlocking the EU General Data Protection Regulation' (*White & Case LLP*, 5 April 2019) <https://www.whitecase.com/publications/article/chapter-12-impact-assessments-dpos-and-codes-conduct-unlocking-eu-general-data> accessed 5 January 2022.
107. GDPR Art. 40.
108. See also GDPR Recitals 77 and 98.
109. ibid Art. 40(2).

Funding

Special thanks to Jeremias Adams-Prassl, Michael 'Six' Silberman, Aislinn Kelly-Lyth, and Sangh Rakshita for their feedback. I acknowledge funding from the European Research Council under the European Union's Horizon 2020 research and innovation programme (grant agreement No 947806).