Offering false security: How the draft artificial intelligence act undermines fundamental workers rights

Aude Cefaliello
Researcher at the European Trade Union Institute (ETUI), Brussels, Belgium

Miriam Kullmann
Associate Professor at Radboud University Nijmegen, Nijmegen, Netherlands

Abstract
In April 2021, the European Commission published its first draft of the Proposal for a Regulation on Artificial Intelligence. Since AI in the work context has increasingly become important in organising work and managing workers, the AI Act will undoubtedly have an impact on EU and national labour law systems. One aim of the proposal is to guarantee ‘consistency with existing Union legislation applicable to sectors where high-risk Artificial Intelligence systems are already used or likely to be used in the near future’, which includes the EU social acquis. It could be argued that ensuring true consistency with EU law means guaranteeing that the way the AI Act will be implemented and applied will still allow the other pieces of EU labour law to fulfil their purpose. It is undeniable that the implementation of the AI Act will overlap with various fields of EU law, especially considering the increasing use of AI technology at work. Thus, this article seeks to identify ways to refine the AI Act, insofar as it impacts work. The contribution discusses the current AI Act as proposed in April 2021, thereby focusing on two particular areas, EU non-discrimination law and EU law on occupational health and safety (OSH), as these two areas are, more or less explicitly, addressed as legal fields in the AI Act. The article starts with taking the perspective of EU labour law influencing the development of AI systems used in the employment context. We argue that providers should respect EU labour law throughout the development of the AI system (section 2). Then, the areas where EU labour law and the AI overlap are identified, thereby viewing it from an employer’s perspective, i.e., the user of the AI system (section 3). Using two specific EU labour law areas (the right not to be discriminated against and the right to healthy and safe working conditions) the article provides a first assessment of how the AI Act might influence work and the regulation thereof (section 4). Finally, the conclusion critically explores whether and to what extent AI in employment situations warrants particular attention (section 5).

Corresponding author:
Miriam Kullmann, Associate Professor at Radboud University Nijmegen, Nijmegen, Netherlands.
E-mail: miriam.kullmann@ru.nl
Keywords
AI Act, EU labour law, occupational health and safety, non-discrimination, worker protection

1. Introduction

On 21 April 2021, the European Commission published its first draft of the Proposal for a Regulation on Artificial Intelligence (AI Act).1 It sets definite parameters for employment and its regulation. Since AI in the work context has increasingly become important in organising work and managing workers, the AI Act will undoubtedly have an impact on EU labour law, as well as Member State labour law systems. One of the AI Act’s key ideas is that ‘the proposal requires full consistency with existing Union legislation applicable to sectors where high-risk Artificial Intelligence systems are already used or likely to be used in the near future’.2 For employment matters in particular, this means the following.

First, relating to the context within which the AI Act has been proposed, that algorithms and their use by employing companies is not new, except that AI in terms of machine learning goes a step further by collecting a huge amount of data, processing that data in real time, and taking decisions in the form of predictions and/or recommendations (while the AI is able to adapt itself based on new data).3 The use of machine learning algorithms will most likely increase in the (near) future.

Second, following the AI Act, AI used in the work context is considered as high-risk and in need of particular criteria to be observed by the stakeholders involved. The question, however, is whether these criteria are enough to seriously and successfully address the dangers stemming from algorithmic decision-making models that are aimed at managing and disciplining workers and at evaluating their work performance, basically reflecting the automation of managerial (or employer) roles in enterprises.4 It is expected that, at one point, almost all sectors of activity will be affected, with all workers being partially, or even fully, managed by an AI in the future. This makes addressing the potential impact of the AI Act in the work context even more important.

It could be argued that ensuring true consistency with EU law means guaranteeing that the way the AI Act will be implemented and applied will still allow the other pieces of currently applicable EU labour law to fulfil their purpose. It is undeniable that the implementation of the AI Act will overlap with various fields of EU law, especially considering the increasing use of AI technology at work. For the regulation of work, this article seeks to identify ways to refine the AI Act, insofar as it impacts work and the EU labour law framework. EU law provides an extensive corpus of rules, yet compared with national labour law systems it is still rather limited, applicable to and relevant for the organisation of work for which AI is or will be deployed in the near future. To mention only the most relevant ones that are part of the EU social acquis: the right not to be discriminated against

1. Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final.
2. COM (2021) 206 final, 4.
3. For an overview of the differences between descriptive, predictive and prescriptive automated decision-making, see, e.g., Johanna Wenckebach and Ernesto Klengel, “Artificial Intelligence, Work, Power Imbalance and Democracy — Why Co-determination is Essential” (2021) 14 Italian Labour Law e-Journal 157.
4. See, for a general overview, Jeremias Prassl, “What if Your Boss Was an Algorithm? The Rise of Artificial Intelligence at Work” (2019) 41(1) Comparative Labor Law & Policy Journal.
based on a limited number of protected grounds (Directives 2000/78/EC, 2000/43/EC and 2006/54/EC); Directives to protect workers’ health and safety (Directive 89/391/EEC and related Directives); the Directive on the consultation and information of workers and their representatives (e.g., Directives 2009/38/EC, 2002/14/EC and 2003/72/EC); and the right of freedom of association, collective bargaining and collective action (Art. 12 and Art. 28 EUCFR).  

Given AI’s increasingly widespread deployment to organise work and manage workers, together referred to as algorithmic management, we understand an AI system that is being used for work purposes very broadly, so as to cover not only decisions that are fully automated but also those to which employers have delegated (specific) managerial decision-making powers. Algorithmic management impacts sectors differently. Therefore, many conventional employment settings, such as warehouses, factories or marketing firms, will be impacted by the increasing usage of AI software to direct, to discipline, and to evaluate workers.

AI has four particular capacities: (1) data collection which, from a technical point of view, can be endless, i.e., it has the capacity to track almost everything 24/7; (2) the processing power and capacity to analyse ‘big data’ for a variety of purposes can take place almost instantly; (3) the capacity of algorithms, based on past patterns combined with some factors chosen by stakeholders, to make predictions and/or suggestions; and (4) the technical capacity to automate decision-making and, to some extent, interact with workers.

All four aspects interact with workers’ interests in two ways. First, the data that is being collected while working, and which is necessary for the ‘development’ or ‘adjustment’ of the AI at the workplace, overlaps with the rights and obligations arising out of the GDPR that limits the collection of ‘fresh data’ endlessly. The choice of data sets will impact the accuracy of the predictions of the AI in specific contexts. For example, the data might have been imported from countries where there are, apart from societal and legal differences, no or fewer restrictions on the collection of data. Moreover, in this context, questions of enforcement and, in particular, the competence of the labour inspections arise, especially with regard to the question of who will sanction employers who do not respect the applicable laws on workers’ data.

Second, the algorithm’s aim(s) will influence the instant processing of data by taking into account the level of ‘weighting’ as attached by humans to some factors in its decision-making process. This certainly impacts the kind of predictions and/or suggestions made by AI and, consequently, the way employing entities will rely on them. As underlined by previous research, the same set of data can be analysed and used in a different way, i.e., different from what the original intention might have been. Data sets, thus, may have different ‘purposes’. The AI Act will regulate both the analysis and usage of data in the context of algorithms impacting the employment relationship by establishing duties and obligations for the provider and the user of AI (i.e., employer/
management). According to these provisions AI should be designed, developed, and deployed in line with the EU fundamental values, such as non-discrimination.\textsuperscript{13}

Having said that, in the following we intend to discuss, from a labour law perspective, the current AI Act as proposed in April 2021, focusing on two particular areas: EU non-discrimination law and EU law on occupational health and safety (OSH). These two areas are, more or less explicitly, addressed as legal fields in the AI Act. That is not to say that collective labour rights are not important, but we will only cursorily address this aspect.\textsuperscript{14} With this in mind, we start with taking the perspective of EU labour law influencing the development of AI systems employed by addressing, in particular, the intended consequences for those providing AI systems, i.e., the providers of the AI systems (section 2). In a next step, we identify the areas where EU labour law and the AI overlap, viewing this overlap from an employer’s perspective, i.e., the users of the AI system (section 3). Taking two specific EU labour law areas, namely, the EU right not to be discriminated against and the right to a healthy and safe work environment, we assess how the AI Act might influence work and workers (section 4). We conclude our contribution by critically discussing whether and to what extent AI in employment situations warrant particular attention (section 5).

\section*{2. The development of AI systems used in employment and the consequences for providers}

\subsection*{2.1. Discrepancies between the provider’s ‘intended purpose’ of the AI system and its ‘reasonably foreseeable misuse’}

One of the key definitions in the AI Act is the ‘intended purpose’ following which the ‘provider’ determines the AI’s purpose, including its specific context and conditions laid down in the instructions for the users as well as in the technical documentation (Art. 3(2) AI Act). Entities can be considered ‘providers’ where they (1) develop an AI system themselves (often also by hiring external experts to assist in the process as well as integrating the views and interests of one of the main customers interested in having the system developed), (2) have an AI system developed with a view to placing it on the market (i.e., where the provider contracts with a business for the development and delivery of an AI system), or (3) are putting it into service under their own name or trademark, whether for payment or free of charge. An AI system is, according to the AI Act, defined as:

\begin{itemize}
  \item a software that has been developed with one or more of the techniques and approaches such as machine learning approaches, logic- and knowledge-based approaches, and statistical approaches, Bayesian estimation, search and optimisation methods, and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.\textsuperscript{15}
\end{itemize}

\textsuperscript{13} Jarrahi et al., “Algorithmic Management in a Work Context” 3; Philippa Collins, Stefania Marassi, “Is That Lawful? Data Privacy and Fitness Trackers in the Workplace.” (2021) 37(1) International Journal of Comparative Labour Law and Industrial Relations. 70.

\textsuperscript{14} Algorithm Watch’s statement also stresses the need for involving workers’ representatives. Algorithm Watch, “Draft AI Act: EU Needs to Live up to its Own Ambitions in Terms of Governance and Enforcement” (Submission to the European Commission’s Consultation on a Draft Artificial Intelligence (AI) Act, August 2021) 9–10.

\textsuperscript{15} Art. 3(1) AI Act.
This definition includes software that is intended for HR purposes, which nowadays goes far beyond the use of online job advertisements, and includes sorting uploaded job applications, filtering out information from the applicants’ CVs and resumés and preparing them for further processing in order to make (automated) statements, which includes predictions, about the (assumed) accuracy of fit of applicants and job offers as well as about the comparability of applicants on this basis. Moreover, an increased use of algorithmic systems is to be expected in the future in the fulfilment of managing tasks in connection with existing employment relationships. With the help of corresponding software, the satisfaction and productivity of employees can be measured and the networking between individual employees and the team composition within companies can be improved. While promising efficiency and saving costs, the (intended purpose of the) AI systems mentioned do not come without risks. While employers as users of AI systems may experience organisational benefits when using specific software which selects the right employees, job applicants, on the other hand, might encounter difficulties in passing the scrutiny of AI systems, especially where the information provided either is seen as not being relevant, or is not recognised as being relevant.  

Acknowledging the risks that may be involved when using AI systems, the AI Act uses a risk classification distinguishing different levels of risk each with particular obligations for providers and/or users of AI systems, including those that are used in a work context. Regarding the latter, an AI system is considered ‘high-risk’ where the AI is intended to be used for (a) recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests and (b) 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 (Annex III, point 4). On close reading, the definition seems to be rather limited. What seem to be excluded from the scope are AI systems that, for instance, have a role in deciding whether an employee’s request for paid annual leave is accepted or whether, and to what extent, an employee will be paid an annual bonus for achieving previously defined goals, while these goals, too, may have been determined by an AI system on an annual basis. Unless such decision-making is part of the monitoring and evaluation of the worker’s performance, it can be argued that all AI systems that affect personal information in the employment relationship should be seen as high-risk. Furthermore, AI systems relating to employment, the management of workers and access to self-employment are so-called ‘stand-alone’ systems which are, under certain mandatory requirements and an ex-ante conformity assessment, permitted on the EU market. As suggested by IndustriALL in its Feedback to the Public Consultation on the AI Act, the nature of the data being potentially collected should also be taken into consideration while determining if the software should be qualified as high-risk or not. Focusing on the data collected would help to better assess the risks of the intended purpose, but also the potential misuse.

16. Miriam Kullmann, “Discriminating job applicants through algorithmic decision-making” (2019) 68 Ars Aequi 45, 53.
17. ETUC, Resolution on the European Strategies on Artificial Intelligence and Data (ETUC Executive Committee, 2 July 2020) <www.etuc.org/en/document/resolution-european-strategies-artificial-intelligence-and-data> accessed 17 March 2022.
18. The purpose of the entire Title III High-Risk AI Systems of the AI Act.
19. IndustriALL Europe’s Contribution to the public consultation on the Proposal for an Artificial Intelligence Act (Brussels, 3 August 2021).
However, the AI Act is only one of the axes of the broader European Digital Agenda. Another one is the European Data Strategy, for which a legislative proposal for a new Data Act on 23 February 2022 has been published. As the AI Act’s explanatory memorandum clarifies, ‘the classification as high-risk does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used.’ Therefore, all obligations attached to high-risk AI systems are only applicable when the intended purpose, as defined by the provider, is used for the recruitment or selection of natural persons or for making decisions on promotion, for the termination of work-related contracts, for task allocation and for monitoring and evaluating the performance and behaviour of persons in such relationships. Some AI systems will easily fall within the category, such as Percolata, which aims to ensure the optimal mix of workers for maximizing sales in every 15-minute slot of the day by allocating schedules on the basis of predictions of demand. Its intended purpose is to allocate tasks to the workers. Nevertheless, the provider’s intended purpose ascribed to the AI system may differ from the employer’s (or user’s) actual use. Where the intended purpose of a high-risk AI system that has already been placed on the market or has been put into service is being substantially modified by the user, the latter will be considered a provider for the purposes of the AI Act (Art. 28(1)(b) AI Act). That also means that the initial provider will no longer be considered a provider and the provider’s obligations will shift to the initial user (Art. 28(2) AI Act).

Even software without an intended purpose to monitor the workers can nevertheless be used to do so. For example, Microsoft Teams can send out weekly MyAnalytics. Reports containing an overview of how much time workers have spent on meetings, writing and emails, or on calls outside of their (agreed) working hours, as well as with whom they are collaborating (or not). This software is a Microsoft-operated business messaging and collaboration platform, seemingly not intended to monitor workers. Yet, it can be combined with other Microsoft software and therefore can be used to monitor workers to see if they respect their working time, how many emails they are opening or the average time of answering them. Existing practices illustrate the discrepancy between the intended purpose of the AI and its (foreseeable?) misuse. For example, in the US, Uber has already implemented some AI with the intended purpose to predict safety incidents by determining the likelihood of the driver being involved in a road accident or an interpersonal conflict. Depending on the outcome of the determination of risk, drivers can face temporary account suspension, which is a form of sanction.

The key question therefore is whether an AI system that is not intended to be used as would be required by Art. 6(2) AI Act in conjunction with Annex III point 4, would fall within the scope of the definition of a high-risk AI system and would therefore be covered by the AI Act. According to the Explanatory Memorandum, “the classification as high-risk does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which that system is

20. See, for a more detailed analysis, Aída Ponce Del Castillo, The AI Regulation: Entering an AI Regulatory Winter? Why an Ad Hoc Directive on AI in Employment is required (ETUI 2021) 2, <www.etui.org/publications/ai-regulation-entering-ai-regulatory-winter> accessed 1 July 2022.
21. COM (2021) 206 final, 13.
22. <www.percolata.com> accessed 1 July 2022.
23. <www.microsoft.com/en-ww/microsoft-365/business/myanalytics-personal-analytics> accessed 1 July 2022.
24. This presupposes, however, that all data are entered into one system or at least that there is one system that has access to all data.
25. Belle Lin, “Uber Patents Reveal Experiments with Predictive Algorithms to Identify Risky Drivers” The Intercept (30 October 2021) <https://theintercept.com/2021/10/30/uber-patent-driver-risk-algorithms> accessed 1 July 2022.
26 On a strict interpretation, then, it might be the case that it would not be covered by the AI Act. This raises two questions: first, what happens in a situation where the AI system is used in accordance with its intended purpose, while at the same time having implications that go beyond the specified purpose? Second, who is going to decide whether the intended purpose is met or not - the provider? One approach would be to use ‘reasonably foreseeable misuse’ to determine the scope of obligations for the provider and the user (i.e., the employer), i.e., the use of an AI system may result from reasonably foreseeable human behaviour or interaction with other systems.

2.2. ‘Reasonably foreseeable misuse’ and ensuring compliance with fundamental rights

Providers are obliged to build into their AI systems the possibility of ‘foreseeable misuse’, as was intended (Art. 9(2)(b) AI Act). That means, in their estimation and evaluation of 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, providers should account for additional uses of AI systems. Moreover, users must be informed about any risks that may result from the intended purpose and foreseeable misuse of the AI system ‘which may lead to risks to the health and safety or fundamental rights’ (Art. 13(3)(b)(iii) AI Act). This is part of the provider’s obligation to adopt a quality management system (Art. 17 AI Act) (see also the following sections).

The crucial point for providers to make sure that AI systems do not violate any laws is when the AI is being designed and developed, as at this stage the providers determine what the AI system’s aim will be and how the system is intended to function in practice to achieve its designated aim. Here, human software developers, together with software architects, and most likely taking into consideration customers’ (and consumers’) interests, are defining and coding the aim(s) of the software and the ways the aim(s) will be achieved. As mentioned previously, this includes determining the relevant data and factors based on which the AI will come to its output, the weight given to these different factors, and the AI’s aim in terms of making predictions and suggestions. Different models are possible, including AI programmes facilitating workers’ well-being or productive goals.27 While the data might be the same for different models, their outcomes may differ. It is the provider who has a particular vision of the AI’s use and aims and who has a say in how the AI system will function and impact the (user’s) work organisation, the latter usually falling within the scope of the employer’s prerogatives. To what extent the user actually has a say in the AI system’s functioning if it is the provider giving it a specific purpose is questionable; even if the provider offers a variety of options of how the AI system can be used through different functionalities, the user may not have a real choice here, except taking it or leaving it.

Therefore, in order to put employing entities as users in a position to make reasoned decisions, full transparency and accessibility (in an understandable manner) on how the AI is conceived by the providers is therefore needed.28 Yet employing entities can be users and providers at the same time, especially where AI systems are being conceived by the employing entity itself. Where an AI system is intended to be used in a work environment, the participation of workers’ representatives should be a necessary requirement to ensure transparency of the AI system’s use because it may

26. COM (2021) 206, 13.
27. See Min Kyung Lee et al., “Participatory Algorithmic Management: Elicitation Methods for Worker Well-Being Models” (AAAI/ACM Conference on AI, Ethics, and Society, 2021).
28. Aída Ponce Del Castillo, The AI Regulation: Entering an AI Regulatory Winter? Why an Ad Hoc Directive on AI in Employment is required (ETUI 2021) 7–8.
impact co-determination rights and obligations, which are created with the intention of giving workers a say in the daily organisation of their work. It is in this context, where recruitment and hiring software as well as other ways to manage the workforce and the legal relationship between employers and employees, where compliance with EU non-discrimination laws must be ensured, e.g., so that the AI is built in a non-discriminatory way and/or will not lead to a discriminatory outcome.

The example of AI software allocating tasks in a warehouse requiring employees to work at a certain pace demonstrates how the design of the software impacts/influences compliance with EU labour law. It is the reason why EU labour law should equally influence (or be taken into consideration during) the design of software deployed at the workplace, such as algorithmic management software. In the majority of cases, the software is clearly programmed to optimise productivity, in favour of the business using that software. Despite the provider’s intended purpose, the user must respect/guarantee the employees’ fundamental right to have decent working conditions, including working time restrictions. Following Art. 6(2)(d) Directive 89/391/EEC, for instance, it is the employer who should adapt the work to the individual, especially as regards the design of work, the choice of working and production methods, with a view, in particular, to alleviating monotonous work and work at a predetermined work-rate and reducing the impact on health. In the current setting, ‘predetermined work-rate’ should be understood as ‘AI-determined work-rate’. Initially, when the Directive was meant to be adopted, the idea was to mitigate or counter the impact of Taylorism with workers being ‘dispossessed’ of their work autonomy. When AI software is allocating tasks, it corresponds to ‘digital Taylorism’, following which workers have no control over the overall process. We would argue that, whenever possible, the provider should dedicate efforts to empower workers by allowing them to make decisions or to make choices. This idea is supported by the European Social Partners’ Framework Agreement on Digitalisation signed in June 2020. Taking into account that ‘due consideration shall be given to (...) the environment in which the system is intended to be used’ (Art. 9(4)), while designing the software, the provider shall integrate the employers’ prerogatives and obligations within its functioning to ensure that modifications can be done once implemented at work.

Overall, the provider’s freedom as to the AI system’s design is limited by the horizontal nature of the AI Act, which requires ‘full consistency with existing Union legislation applicable to sectors where high-risk AI systems are already used or likely to be used in the near

29. For example, in the leaked proposal on the sustainable use of plant protection products (repealing Directive 2009/128/EC), which is also a horizontal regulation overlapping with parts of EU labour law (e.g., OSH), recital 25 explicitly refers to the OSH Directives for the assessment of the risks. A similar wording could be recommended for the AI and would read as follow: ‘To the extent that the deployment and implementation of the AI software require the setting of minimum health and safety requirements at the workplace, covering the risks arising from exposure of workers to such software, as well as general and specific preventive measures to reduce those risks, those measures are covered by Directive 89/391/EEC (and all specific/individual directives).’

30. Christophe Degryse, Shaping the World of Work in the Digital Economy (ETUI 2017) 2.

31. ‘The potential tensions between respect for human autonomy, prevention of harm, fairness and explicability of decision making should be acknowledged and addressed. Deployment of AI systems: should be safe, ie, it should prevent harm. A risk assessment, including opportunities to improve safety and prevent harm such as for human physical integrity, psychological safety, confirmation bias or cognitive fatigue should be undertaken.’ European Social Partners Framework Agreement on Digitalisation <www.etuc.org/system/files/document/file2020-06/Final%202022%2006%2020_Agreement%20on%20Digitalisation%2020.pdf> accessed 1 July 2022. For an analysis of the Framework Agreement, see David Mangan, “Agreement to Discuss: The Social Partners Address the Digitalisation of Work” (2021) 50 Industrial Law Journal 689. The Framework Agreement has also
future.’ The Explanatory Memorandum mentions the following sources with which compliance must also be ensured: the EUCFR and existing secondary EU law on data protection, non-discrimination and gender equality. Yet, in line with the Explanatory Memorandum cited earlier, we suggest that the sources mentioned should only be seen as examples and that AI systems that are intended to be used in a work context as defined in Annex III point 4 need to guarantee compliance with the full EU social acquis.

2.3. Design and choice of the data set: not neutral variables

There are AI systems that are being developed and then placed on the market and, from time to time, are being updated. However, there are also AI systems that, once placed on the market and being used, automatically update or adjust themselves based on new data collected, probably leading to different predictions and/or recommendations than before (so-called machine learning). Yet, despite the fact that machine learning is the basis for an AI system, it does not seem that the initially aim of the AI system defined by the provider, per definition, will change with the input of new data. It seems that only the kind and amount of data that is being processed, to make the decision-making more accurate and fitted to a specific situation, has changed. This reflects the situation that the initial AI system’s settings will be static, a point that regulation may be capable of addressing. More challenging then seems to be, from a regulatory point of view, the new data that will be used by the AI system and the outcome of the decision-making processes. Nevertheless, the issue of machine learning raises two particular issues: first, as to the way the data is collected from work and/or workers and hence processed by the AI system and, second, as to the access of the provider to these data collected from work and/or workers to fulfil their requirements as to the ‘post-market monitoring’ of the AI (Art. 17(1)(h) in conjunction with Art. 61 AI Act). In this context, three sources of data are relevant: digital information (i.e., information available online); sensors transmitting information; and employee self-tracking. It should, however, be stressed here that

...even where information is collected and stored in anonymized form, as information is increasingly organized in machine-readable formats, data sets from different sources can – at least in principle and subject to data processing consent and privacy laws in jurisdictions such as the European Union – easily be combined to build large employee databases, and – again, at least in principle – quickly identify individuals within a firm.

Training and validation data sets, in combination with the provider’s intended purpose and the foreseeable misuse, are crucial for the development of the AI system and will influence the way the AI will provide predictions and recommendations. Thus, depending on the AI system’s intended purpose, it might be argued that training and validation data should be different depending on the specific sectors of employment in which the AI systems are intended to be used. Indeed, there are substantial differences with regard to the kind of work being performed within these sectors, and, moreover, different sectors have a different gender balance, with IT being more male-dominant and care work more female-dominant.

32. COM (2021) 206 final, 4.
33. Jeremias Prassl, “What if Your Boss Was an Algorithm? The Rise of Artificial Intelligence at Work” (2019) 41(1) Comparative Labor Law & Policy Journal, 134.
34. Ibid., 135.
At the same time, if the AI system has been developed with data collected from a continent outside the EU, for instance the US, and will be used for recruitment and hiring purposes in an EU Member State, the question is whether that data, which is likely predominantly based on the composition of the American society, is actually representative of the European (sectorial) workforce and, in some cases, the use of data of EU citizens by parties in third countries may even not be permissible in the EU setting.\(^{35}\) Also, depending on how old the data is, outdated perceptions and biases may be reflected in the AI system’s decision-making.\(^{36}\) Providers of AI systems should be asked to articulate the composition of the systems, as these elements might influence the users.

### 2.4. Managing the risks of high-risk AI systems and post-market surveillance

Providers of AI systems, as well as distributors, importers, users or other third parties that can be considered as providers need to establish, implement, document and maintain a risk management system in relation to high-risk AI systems (Art. 9(1) AI Act). This system shall consist of a continuous iterative process run throughout the AI system’s entire lifecycle, requiring regular systematic updating (Art. 9(2) AI Act). This includes any residual risk associated with each hazard as well as an assessment of whether the overall residual risks of the high-risk systems are judged acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or, if not, whether there is reasonably foreseeable misuse. With a view to eliminating or mitigating risks related to the use of high-risk AI systems, due consideration should be given to the technical knowledge, experience, education and training that is expected from the user, and the environment in which the AI system is intended to be used (Art. 9(4) AI Act).

Here, the conception and the definition of the ‘intended purpose or under conditions of reasonably foreseeable misuse’ is crucial because it will determine which AI systems are subject to such a risk assessment or not. A similar issue arises in respect of access to data from work to have an accurate risk management system once the AI is used and implemented at work. This raises some concerns, namely, that the technical knowledge, experience, education and training of the user, and the environment in which the system is intended to be used will influence the way risks will be eliminated or reduced. If this is applied to work, does it mean that depending on the sectors, the risks should not be assessed in the same way? Also, how does the provider assess the expected user? Will they distinguish between a manager in a multinational and the director of an SME? Also, the phrase ‘due consideration shall be given’ creates some concern. Does it mean there will be consultation with the social partners when the intended purpose of an AI is to be used at work? Or is the provider simply ‘considering’ some elements on its own without any evidence that it corresponds to the reality of work? Additionally, the reference to ‘technical knowledge’ leads to the question of whether it means that the usage of high-risk AI is allowed as soon as the expected user is AI-literate. It can also be seen as a way of transferring the responsibility

---

35. See, for the latter, the *Schrems* decisions in which the CJEU dealt with the question whether a third country would be capable of ensuring an ‘adequate level of protection’, i.e. ‘a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter’ (*Schrems I*, para 73): Case C-362/14 *Schrems I* ECLI:EU:C:2015:650 and Case C-311/18 *Schrems II* ECLI:EU:C:2020:559.

36. Raphaële Xenidis and Linda Senden, “EU Non-discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges of Algorithmic Discrimination” in Ulf Bernitz, Xavier Groussot, Jaap Paju and Sybe de Vries (eds), *General Principles of EU Law and the EU Digital Order* (Alphen aan den Rijn, Kluwer Law International 2020) 154.
and the risk associated with the usage of high-risk AI. Also, high-risk AI systems that continue to
learn after being placed on the market or put into service shall be developed in such a way to ensure
that possible biased outputs due to outputs used as an input for future operations (‘feedback loops’) are duly addressed with appropriate mitigation measures (Art 15(3) AI Act).

Providers of AI systems have to proactively collect and review experience gained from the use of AI systems placed on the market or put into service to identify any situations where corrective or preventive actions would be needed. Post-market monitoring systems should be proportional to the nature of the AI technologies and the risks of the high-risk AI system. Moreover, the system has to actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements (Title III, Chapter 2 AI Act). It should be underlined here that risks should be identified and assessed accurately. But what does proportionate to the nature of the AI actually mean?

A question arises in respect of the collection and communication of data collected at work once the AI is used by the employer. Is there an obligation for the user (i.e., the employing entity) to communicate the data collected? Following the GDPR, it might indeed be the case (see Art. 13), but then the data collection at work should be discussed with the social partners or other workers’ representatives. Again, the way data is collected and communicated to a third party can create stress and anxiety at work. If it is not an obligation and the employer does not provide the data to the provider, does it place the provider outside of the liability ‘loop’ or scope in case of an accident?

2.5. Over-reliance on providers’ self-assessment: protections of health and safety and non-discrimination rights without safeguards

The AI Act pursues a high level of protection of the applicable health, safety, and fundamental rights under Union law, aimed at guaranteeing that AI systems are safe. However, as the analysis below will stress, most of the provisions aiming to provide better security fall short when examined in detail (or fail the security assessment when testing against the reality of the workplace dynamic). We will focus on three mechanisms of security, for which there is a high-risk that the AI Act will not deliver on its promises: (1) conformity assessment, (2) post-market surveillance and (3) reporting mechanisms.

The first attended layer of security is the conformity assessment. When AI software is considered high-risk, the provider should meet a certain number of requirements (see Art. 16) to prove that the software can be safely used. Amongst the obligations listed in Art. 16 AI Act, the providers of high-risk AI systems shall ensure that the high-risk AI system undergoes the relevant conformity assessment procedure before being placed on the market or put into service. The AI Act provides extensive details on the notification of authorities and bodies that are supposed to act as safeguards of the high-risk AI system. However, Art. 43(2) AI Act introduces an exemption for high-risk software intended to be used at work.

37. Assuming, however, that the user (i.e., the employing entity) can be considered as a controller here, which means that he determines the purposes and means of the processing of personal data. This might increase the risk of misunderstanding or failing to understand the terminology of the differing regimes. Similar to the GDPR, where an employer is a processor, he is a user under the AI Act.
Indeed, for this software, providers have to follow the conformity assessment procedure based on an internal control that is to be conducted, but, strangely enough, this control does not provide for the involvement of a notified body. The conformity assessment procedure based on an internal control requires the provider to self-assess its own quality management system (Art. 17 AI Act) and make sure that the design and development process of the AI system is consistent with the technical documentation. The quality management system includes the risk management system referred to in Art. 9 AI Act and the procedures related to reporting serious incidents and malfunctioning (Art. 62 AI Act).

In sum, it means that the same entity assesses the risks of the AI system and checks whether the AI system is safe, without the mandatory involvement of any other stakeholders. Moreover, it means that in addressing the potential risks of high-risk AI intended to be used at work, the European Commission seems to consider it safe to rely on self-assessment and self-regulation without the involvement of a third party, even if (or despite) the involvement of national authorities will be established for other high-risk systems. In a critical assessment of the AI Act, Ponce Del Castillo has argued that these requirements are weak and insufficient and should be replaced by a third-party conformity assessment. Additionally, the assessment of high-risk AI systems at work does not take into consideration the possibility of combining multiple AI which creates different risks to those associated with AI systems individually. This position is echoed by the opinion paper of the European Economic and Social Committee.

Self-governance on AI has been criticised. Instead of internal governance, Yeung et al. recommend a legally mandated external oversight by an independent regulator with appropriate investigatory and enforcement powers to address the ineffectiveness of the prevailing self-regulatory approach to ‘ethical AI. Ultimately, they recommend an alternative governance model. According to these authors, regulatory authorities should have appropriate powers of investigation and enforcement and provide for input from both technical and human rights experts, on the one hand, and meaningful input and deliberation from affected stakeholders and the general public, on the other. The same authority then could address and receive the complaints associated with redress mechanisms for organisations and citizens who have suffered harm from any AI system, practice, or use that falls within the scope of the AI Act, as recommended by the European Economic and Social Committee.

The second layer of safety is the post-market surveillance system. But this presents another serious concern with the AI Act, in particular, regarding the reporting of serious incidents and malfunctioning procedures (Art. 62 AI Act). Similar to other definitions in the AI Act, the ‘serious incident’ (Art 3(44) AI Act) definition is too restrictive and gives a false or deceptive feeling of safety. Currently, a ‘serious incident’ means any incident that directly or indirectly leads, might have led or might lead to (a) the death of a person or serious damage to a person’s health, to property or the

38. Aida Ponce Del Castillo The AI Regulation: Entering an AI Regulatory Winter? (2021) ETUI Policy Brief. 3.
39. Ibid., 5: ‘A harmonised assessment framework must be developed to avoid a multiplicity of approaches and, finally, where a user puts together several AI systems, the assessment should not only cover each individual system but also them all in combination.’
40. Catelijne Muller, Opinion AI/Regulation (European Economic and Social Committee, INT/940, 2021).
41. Karen Yeung et al., “AI Governance by Human Rights-Centered Design, Deliberation, and Oversight: An End to Ethics Washing” in Markus D. Dubber, Frank Pasquale and Sunit Das (eds), The Oxford Handbook of Ethics of AI (Oxford, Oxford University Press 2020) 79.
42. Catelijne Muller, Opinion AI/Regulation (European Economic and Social Committee, INT/940, 2021).
environment or (b) the serious and irreversible disruption of the management and operation of critical infrastructure. One might argue that this conception of serious incident is too narrow, considering that most of the risks caused by AI in platform work and traditional employment settings are linked with psychosocial rather than physical risks.43 A mistake or the misusage of the AI will lead to death or serious accident only on rare occasions. It might be the case that the risk will materialise in some sectors (e.g., the construction sector or technologies used on the road), but otherwise, constant monitoring will result in stress, anxiety, and potentially burnout or work exhaustion. In a similar vein, where an AI system results in a decision that (directly or indirectly) discriminates against a worker, this will hardly result in the classification of the situation as a serious incident following which a report must be filed.

Moreover, it is argued here that the serious incident mentioned under (b) should be replaced by a serious disruption of the management and operation of critical infrastructure. The impact of an AI system on work organisation might qualify as a serious disruption, but adding the irreversible criteria to it will limit its scope. The disruptive effect of the AI on work organisation would be more subtle than irreversible change causing the death of a person.

For example, the malfunction of software such as Driveri, intended to improve health and safety on the road, is more likely to lead to a serious accident endangering workers’ physical condition on the road than Cogito. Cogito is software that provides ‘real-time emotional coaching’. It constantly monitors workers during calls, and provides them with visual cues to adjust their performance. Cogito might cause anxiety and stress, but it is less likely that it will result in a fatal accident. One might argue that if a worker ‘subject to’ Cogito monitoring experiences depression or burnout, it could be indirectly linked to the serious psychological damage suffered by the worker. The scope of serious incidents and malfunctioning is only one facet of the problem.

Finally, some concerns also relate to the third layer of safety, the reporting mechanisms. Currently, even if the use of an AI system causes the death of a worker, the reporting mechanism still relies on self-assessment and self-reporting by the provider. Indeed, according to Art. 62(1) AI Act, providers of high-risk AI systems that are placed on the Union market have to report any serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where the incident or breach occurs. Such notification shall be made immediately after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and in any event, no later than 15 days after the provider becomes aware of the serious incident or of malfunctioning.

In theory, all breaches of EU anti-discrimination and OSH law have to be reported to the market surveillance authorities. However, providers will only report a problem if they identify a causality between the incident and the use or functioning of the AI system. The likelihood that the provider will self-identify such a link is expectedly low.44 Additionally, the notification should made be once the provider becomes aware of the serious incident or malfunctioning, meaning that the employer/user should communicate such information. This aspect does not take into consideration the employment law dynamic. If the employer, acting as a user of the AI system, reports that there has been a serious incident at work due to the use of the AI, he might be engaging with or

43. Adrian Todoli-Signes, “Making Algorithms Safe for Workers: Occupational Risks Associated with Work Managed by Artificial Intelligence” (2021) 27 Transfer: European Review of Labour and Research 454.
44. On the weakness of self-reporting mechanisms as law enforcement, see Heiko Gerlach, “Self-reporting, investigation, and evidentiary standards.” (2013) 4 The Journal of Law and Economics 56, 1061–1090.
recognising his own responsibility in the incident. Thus, to ensure and to guarantee that serious incidents or malfunctioning will be effectively addressed, it is necessary to include in the AI Act reporting mechanisms for the workers or their representatives to a third-party agency.

To conclude this section, even if the AI Act is a technical regulation or an instrument of EU technical standardisation, when an AI system might impact the employment relationship, the social acquis embedded in EU labour laws should influence the development of AI systems, which would particularly impact providers. To ensure that workers are adequately protected, it is important to understand reasonably foreseeable misuse broadly to determine the scope of obligations for the provider and the user (i.e., the employer). Moreover, the provider’s freedom in designing the AI systems should be limited by existing Union legislation applicable to sectors where high-risk AI systems are already used or are likely to be used in the near future.45 Here, we suggest that AI systems that are intended to be used at work need to guarantee compliance with the EU social acquis. Regarding the content/substance of the AI system, and to guarantee that recommendations provided by the AI system are suitable for the workplaces where it will be deployed, despite arguments relating to proprietary issues, providers of AI systems should particularise the composition of the systems, as these elements might influence users (e.g., the employer and the workers/workers’ representatives). Part of the way the AI systems will be implemented in the workplace should also cover the way data is collected and communicated to a third party (i.e., a provider). Clarifications are needed on whether the user’s (i.e., the employer or worker) refusal to deliver the data to the provider places the provider outside of the liability ‘loop’ or scope in case of an accident. Indeed, the use of AI in the workplace can create breaches of EU law. If the Commission would like a high level of protection for health, safety, and fundamental rights, including non-discrimination rights, and to guarantee that AI systems are safe, it is necessary to include in the AI Act reporting mechanisms for the workers or their representatives to an external and independent third-party agency. This is even more important where the question of compliance with particular EU labour rights is concerned. As the AI Act lacks a proper preventive AI impact assessment to assess whether and to what extent non-discrimination and/or OSH rights are being violated, an independent authority with repressive and monitoring role appears to be the absolute minimum required. It is in line with this that the following section will address the influence of the AI Act on EU non-discrimination and OSH law.

3. The influence of the AI Act at work: ensuring agency to workers and their representatives

3.1. The influence of the AI Act on EU non-discrimination law

Algorithmic decisions have the appearance of an objective and unquestionable procedure, but this is a misconception.46 Algorithmic-based management, for instance, can also lead to insidious forms of discrimination by hiding the programmers’ implicit, and perhaps even explicit, bias behind a technological ‘objective’ façade.47 This is also acknowledged by the AI Act through classifying AI systems in the context of employment as high-risk. AI systems already make inferences

45. COM (2021) 206 final, 4.
46. Miriam Kullmann, “Platform Work, Algorithmic Decision-Making, and EU Gender Equality Law” (2018) 34 International Journal of Comparative Labour Law and Industrial Relations 1, 9.
47. Valerio De Stefano, Simon Taes, “Algorithmic management and collective bargaining” (2021) ETUI Foresight Brief 2.
through the data they collect and express a ‘judgment’.\textsuperscript{48} Often, users do not know how inferences are made and why the algorithms suggest certain decisions, especially when users/managers rely on non-proprietary software and programmes (not in-house software).\textsuperscript{49} Those challenges are particularly related to the complexity, opaqueness, ubiquity and exclusiveness of AI systems.\textsuperscript{50} As mentioned earlier, the AI Act requires, in the first place, providers but also users, to ensure ‘full consistency’ with, \textit{inter alia}, EU law on non-discrimination. In fact, according to the Explanatory Memorandum, the AI Act is intended to complement existing EU law on non-discrimination by giving specific requirements aimed at minimising ‘the risk of algorithmic discrimination, in particular in relation to the design and the quality of data sets used for the development of AI systems complemented with obligations for testing, risk management, documentation and human oversight throughout the AI systems’ lifecycle’.\textsuperscript{51} Given the AI systems’ potential, through the perpetuation of historical patterns of discrimination, to ‘impact future career prospects and livelihoods’, all AI systems ‘used in employment, workers’ management and access to self-employment’ are considered high-risk.\textsuperscript{52}

The starting point of the AI Act is that all such AI is high-risk, and therefore subject to a particular set of (additional) rules. Under existing EU non-discrimination law, employers already are required not to discriminate against (prospective) employees on a limited set of protected grounds (sex, religion or belief, disability, age, sexual orientation, ethnic origin).\textsuperscript{53} That is, ideally employers will have adapted their and their customers’ preferences so as to align them with existing non-discrimination law. This, however, requires the employers and perhaps also customers to be aware of (potential) discrimination or biases. Where this is already difficult to find in an analogue world, it might be even more hard to find in an increasingly digitalised labour market in which decision-making (or parts of it) is automated. In particular, where discrimination does not explicitly take place based on a legally defined protected ground, but by a proxy, that is when the ‘law seeks to prohibit discrimination on the basis of traits containing predictive information that cannot be captured more directly within the model by non-suspect data’.\textsuperscript{54}

This question is even more important in situations where the user’s actual use of the system deviates from the AI system’s intended purpose. Following Art. 29(1) AI Act, users are obliged to use AI systems ‘in accordance with the instructions of use accompanying the systems’. That does not, however, release employers as users from their existing obligations under EU non-discrimination law, as paragraph 2 specifies. In cases where the user has control over the input of data, he must ‘ensure that input data is relevant in view of the intended purpose of the high-risk system’ (para. 3). Should any risks appear, the user has to inform the provider and suspend its use, but only in the case that it concerns a risk within the meaning of Art. 65, referring to a ‘serious incident’ or a ‘malfunctioning within the meaning of Article 62’. Malfunctioning is defined as ‘a breach of

\begin{itemize}
\item \textsuperscript{48} Cathy O’Neil, \textit{Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy} (New York, Broadway Books, 2016).
\item \textsuperscript{49} Frank Pasquale, \textit{The Black Box Society: The Secret Algorithms That Control Money and Information} (Cambridge, Massachusetts, Harvard University Press 2015).
\item \textsuperscript{50} World Economic Forum, \textit{How to Prevent Discriminatory Outcomes in Machine Learning} (Global Future Council on Human Rights 2016-2018, 2018) 7.
\item \textsuperscript{51} COM (2021) 206 final, 4.
\item \textsuperscript{52} COM (2021) 206 final, 26.
\item \textsuperscript{53} Notably Directives 2000/78/EC, 2000/43, 2006/54.
\item \textsuperscript{54} Anya ER Prince and Daniel Schwarcz, “Proxy Discrimination in the Age of Artificial Intelligence and Big Data” (2020) 105 Iowa Law Review 1257, 1263.
\end{itemize}
obligations under Union law intended to protect fundamental rights’. In that case, providers, if they have been informed by employers as users, should report the malfunctioning to the market surveillance authority of the relevant Member State.

3.2. In need of high-data quality and the use of special categories of personal data

As to the development of AI systems, Art. 10(1) AI Act requires high-risk AI systems which make use of techniques involving the training of models with data to be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5. According to Art. 10(3) AI Act, training, validation and testing data sets have to be relevant, representative, free of errors and complete. Moreover, the data needs to have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination of thereof.

High data quality appears to be the main concern of the AI Act to ensure that a high-risk AI system does not become the source of prohibited discrimination. As to high data quality, the AI Act also suggests that special categories of personal data, as mentioned in Art. 9 GDPR, ‘as a matter of substantial public interest’ should be used ‘to ensure the bias monitoring, detection and correction in relation to high-risk AI systems’ (recital 44). Data mentioned within the meaning of Art. 9 GDPR means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation, some of which reflect the grounds based on which employees may not be discriminated against. In principle, processing special categories of personal data is not permitted, unless one of the following exceptions applies: (1) if (prospective) employees give their consent (Art. 7(3)(a) GDPR), (2) if employers/users exercise their rights and obligations under labour or social law and fulfil their legal obligations (Art. 7(3)(b) GDPR) or (3) if (prospective) employees make personal data publicly available to others. However, with regard to the recruitment process, the Article 29 Working Party warns employers not to use data that can be accessed via social media, for example, too lightly as the (private) information shared may not always be relevant to the job advertised or the fulfilment of the employment contract. 55 Applying the high data quality requirement then reflects the second exception where employers are making sure that they do not violate labour law, including the right of non-discrimination. Generally, however, data processing must be adequate, relevant and limited to what is necessary in relation to the purpose (Art. 5(1)(c) GDPR) as well as accurate and kept up to date (Art. 5(1)(d) GDPR).

Where a US-based business is specialised in developing AI systems that promise to find the most suitable employees in finance, for instance, and this system has been developed, trained and tested with datasets that represent American society, can it be said that such an AI system which might be used by an employer based within the EU, and whose workforce might not reflect the different EU societies, is of high quality? Or does high quality data mean that an AI system that has been developed with the aim of automating hiring and recruiting decisions should be adapted depending on the composition of the society to which the AI system will be applied? Following recital 44,

55. Article 29 Working Party, Opinion 2/2017 on Data Processing at Work, 11.
‘[t]raining, validation and testing data sets should be sufficiently relevant, representative and free of errors and complete in view of the intended purpose of the system. They should also have the appropriate statistical properties, including as regards the persons or groups of persons on which the high-risk AI system is intended to be used. … training, validation and testing data sets should take into account … the features, characteristics or elements that are particular to the specific geographical, behavioural or functional setting or context within which the AI system is intended to be used’ (see also Art. 10(4) AI Act).

Article 10(1) on data and data governance specifies quality criteria that high-risk AI systems must meet, which includes making relevant design choices and taking relevant data preparation processing operations (such as annotation, labelling, cleaning, enrichment, aggregation), formulating relevant assumptions, prior assessment of the availability, quantity, and suitability of the data sets, examining data in view of possible biases, and identifying any possible data gaps and how these will be addressed. How these criteria can be mobilised to make an assessment of the AI system as to its discriminatory potential is not further addressed in the proposal. Hence, what is lacking here, according to our opinion, is a so-called AI impact assessment containing questions that providers and/or users have to answer before an AI system is launched. Through such an AI Impact Assessment it would be possible, first, to raise awareness of the discriminatory potential of AI systems and in particular the data (sets) they are running on and, second, to prevent non-compliance with EU non-discrimination law.

All this is important because the provider must design and develop an AI system so as to ensure that they operate sufficiently transparently to enable users (i.e., employers) to interpret the AI system’s output and use it appropriately. Instructions by the provider should support users in this. These instructions, notably, must identify the characteristics, capabilities and limitations of performance of the high-risk AI system (Art. 13(3)(b) AI Act), which includes the system’s ‘intended purpose’, its level of accuracy, robustness and cybersecurity (see also Art. 15 AI Act), any known or foreseeable circumstance, in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, its performance regarding the persons or groups of persons on which the AI system is intended to be used and, when appropriate, specifications for the input data or any other relevant information in terms of data sets used. What stands out here is that the provider’s internal control within the meaning of Annex VI is said to be sufficient (Art. 16(e), Art. 19, Art. 43(2) AI Act). This internal control involves three steps, namely, that the provider (1) verifies that the established quality management system is in compliance with the requirements of Art. 17 AI Act, (2) examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements set out in Title III, Chapter 2 and (3) verifies that the design and development process of the AI system and its post-market monitoring as referred to in Art. 61 AI Act is consistent with the technical documentation. Nobody shall be notified nor involved in the control.

The proposed procedure/system is a missed opportunity for several reasons. As underlined previously, providers are tasked with both designing AI systems, as well as ensuring these systems comply with the applicable law. These obligations might create (or increase) the power imbalance where workers are unlikely to have been informed about the actual impact and (dual) purpose of the AI system used. Meanwhile, these same workers are left to take steps to counteract discriminatory outcomes by taking a court case should they wish to have their right not to be discriminated against - a right directly derived from EU law - protected by a (national) court. While internal control is an important instrument, this internal control should be part of the normal procedure before an AI
system is put on the market rather than being seen as the only monitoring opportunity before the AI system is used. By leaving the conformity assessment to the provider, workers will, should they suspect the AI system to be discriminatory, need to turn to the user/employer and/or the provider. While at the national level a labour inspectorate or another public authority may have the authority to enforce compliance with EU non-discrimination law, this occurs mostly \textit{ex post} rather than \textit{ex ante}. Given the enormous impact AI systems may have, including preventing job applicants from accessing the labour market through a job in order to make a living, a preventive enforcement mechanism is recommended here.

3.3. \textit{Interconnection between the AI Act and occupational safety and health legal framework}

The usage of algorithmic management software at work has proven to negatively impact workers’ health and safety. Continuous monitoring via wearables increases work stress while affecting productivity.\textsuperscript{56} The way the algorithm allocates tasks and tracks workers affects work organisation and negates workers’ right to appropriate breaks, leading to severe physical and psychological stress. However, research also has shown positive effects of using the concept of ‘participatory algorithmic governance framework’, using a model considering workers’ well-being.\textsuperscript{57} Directive 89/391/EEC is the cornerstone of the EU OSH legal framework, providing a general employer obligation to ensure the safety and health of workers in every aspect related to work via the application of the principles of prevention. The Directive adopts a worker-centric approach, with the employer obliged to consult and to inform the workers or their representatives. It also provides workers or their representatives with the right to appeal to the competent authority if they consider that OSH prevention is inadequate. Workers and their representatives are an important part of the elaboration and the implementation of the preventive measures at work.

Even if the Framework Directive was adopted thirty years ago, it contains provisions that are relevant for the implementation of (high-risk) AI at work. When an employer considers integrating an AI software at work, he should evaluate the extent to which the algorithmic management’s use, or its integration within the working environment, will impact workers’ health and safety. According to Art. 6(2) Directive 89/391/EEC, the employer shall eliminate or reduce the risk by adapting the working methods with a view to alleviating monotonous work and work at a predetermined work-rate, as part of a coherent overall prevention policy that covers technology. To base his assessment on the potential risks of the AI, the employer will probably take into consideration all the risks identified by the provider on the occasion of the risk management evaluation and assessment, which should be communicated to the employer as a user of the AI (Art. 13(3)(iii) AI Act). Indeed, according to Art. 9(2)(a) AI Act, the provider should have identified and mitigated the known and foreseeable risks associated with the AI system. Additionally, the employer, as a user of AI, should have been informed of the residual risks of the AI system (Art. 9(4) AI Act). Therefore, the employer should consider the providers’ risk assessment to evaluate the potential impact of the AI system at work.

\textsuperscript{56} Jeremias Prassl, “What if Your Boss Was an Algorithm? The Rise of Artificial Intelligence at Work” (2019) 41(1) Comparative Labor Law & Policy Journal, 130.
\textsuperscript{57} Min Kyung Lee et al. “Participatory Algorithmic Management: Elicitation Methods for Worker Well-Being Models” (2021) Presented at the AAAI/ACM Conference on AI, Ethics and Society.
The requirement to have a ‘significant harmful impact on health and safety’ might be too restrictive and may lead to the exclusion of AI systems being qualified as high-risk even if they represent a danger to the workers.\(^5\) Indeed, a significant part of the harmful effect on workers is psychological (e.g., stress due to monitoring). The harmful impact does not appear immediately; it is a gradual process. Also, the severity of the harm might vary from one worker to another. Therefore, the phrasing should be replaced by ‘potential significant harmful impact on health and safety’, even if it leads to restrictions on international trade. Indeed, the improvement of workers’ safety, hygiene and health at work is an objective which should not be subordinated to purely economic considerations.\(^5\)

As explained in the first part of this article, the concept of intended purpose also raises the question as to the scope of the definition of the high-risk AI. Art. 3(12) AI Act defines ‘intended purpose’ as the use for which an AI System is intended by the provider. Some software might have an impact at work without intending to simply because it is used in an employment context featuring an imbalance of powers.\(^6\) We argued previously that providers should take into consideration employer’s duties while designing the AI and foreseeing its deployment at work. Similarly, if the AI system is intended to be used at work, the provider cannot ignore the impact on workers’ health and safety. The provider should also take into consideration that the AI should be designed with a view to alleviating monotonous work and work at a predetermined work-rate and to reducing their effect on health.

Indeed, the impacts on operational work processes or occupational health and safety must be explicitly considered in the risk management system required for high-risk AI systems. Providers can contribute to a better and fairer application of AI at work when they develop the software. For example, when they programme AI to allocate tasks, they should guarantee that the goals are realistic - and not necessarily aiming at economic optimisation. Also, they should develop systems where these goals can be adjusted to individual capacities while avoiding risks of retaliation. For example, providers could cross or combine the allocation of tasks (and target goals) with analysis of vital signs (e.g., heart rate, skin temperature) and environmental variables (e.g., movements). The idea would be that whenever the vital signs or environmental variables signal that the worker is tired, the AI should adjust the allocation and/or organisation of work to allow the worker to be safe. An option could be given to the worker to either reduce pace for the next two hours or take a break. Rather than having a warning that the worker is not quick enough to fulfil the predetermined goal, the AI should not pressure the worker further and should adjust the goal to a human pace. The average handle time or target should be left to collective bargaining and discussion at organisational level. The provider should not be in a position to set target goals that are a matter of work organisation. It should develop the AI in such a way that this kind of variable can be adjusted at work level.

However, such an approach means that data on workers’ vital signs might be accessible by the employer, and it represents a significant risk if unregulated.\(^5\) Thus, the employer should access

---

58. Recital 27 AI Act.
59. Recital 13 Directive 89/391/EEC.
60. See for more details Philippa Collines, Joe Atkinson, “Labour Values and Technology at Work” (2021) Presented at the 5th Labour Law Research Network Conference.
61. If the vital signs do not allow the recognition or identification of an individual, they cannot be considered to be biometrics. However, vital signs should fall under Art. 4(15) GDPR data concerning health, meaning personal data related to the physical or mental health of a natural person. If the worker has given explicit consent to the processing of those data,
workers’ data only when the data are aggregated and anonymised; otherwise, there is a risk that the
worker will be penalised for being too slow. Similarly, all the data collected from work should be
aggregated and anonymised before being communicated to the provider in the context of the post-
market surveillance (Art. 61(1) AI Act).

To conclude this section, AI systems have an impact on areas such as EU non-discrimination and
OSH law, yet following the previous discussion, it is difficult to see how this part of the EU social
acquis has been seriously taken into account in the AI Act as proposed in April 2021. With that, we
do not mean to argue that the EU should regulate in detail on issues of AI that touch upon EU non-
discrimination law and OSH law. Yet through this proposal and through a thorough assessment of
the fundamental rights implications of AI systems, ambiguities could have been removed, if this can
be regarded as an objective at all, of course. It is, as we have shown, clear by now that AI can be
discriminatory and can be detrimental to workers’ health. A crucial factor in all this, it seems, is the
quality of the data that is being used in the course of developing and applying AI systems. It is this
factor that is, curiously, only cursorily addressed in the proposed AI Act, either because it is left to
the GDPR or because the lack of clarity in this respect has been driven by another factor.

4. Concluding remarks: what next?

The article’s aim was to examine the current AI Act as proposed in April 2021 from the perspective
of EU labour law, focusing, in particular, on the fields of non-discrimination and health and safety at
work. The main argument is that the AI Act does not exist as a stand-alone piece of legislation and
should be considered carefully in respect of-with the existing EU labour legislation. The
Commission stressed the importance of developing the AI Act in coherence with the New
Legislative Framework (e.g., Machinery Regulation). However, we argued that other legal fields
should be taken into account i.e., labour law. We have demonstrated the potential implications
of the implementation of AI systems in the employment context, and the interconnection
between this Act and existing EU labour law. Due to the specificities of the work relationship
(i.e., the imbalance of power), the providers should be aware of and partly responsible for the
effect that their software can have in this particular context.

We highlighted four essential concerns about the AI Act in respect of its application in work-
related contractual relationships. Under its current form, the AI Act restraints or confines the qualifi-
cation of high-risk software only when providers determine the AI is intended to be used in
employment, workers’ management and access to self-employment for the recruitment and selec-
tion of persons, for task allocation, monitoring and the evaluation of workers. As demonstrated,
there might be a difference between the provider’s intended use and the employers’ use of a soft-
ware. We recommend that even if software is not intended to be used for monitoring workers, the
simple fact that it is foreseeable that this software will be deployed in a work-related contractual
relationship should be enough to qualify it as high-risk.

Additionally, to guarantee the effective application of labour law at work, the providers of AI
software intended to be used at work should respect the freedom of the social partners in the imple-
mentation and deployment of the software. Therefore, the providers should guarantee: (1) full

or if the employer justifies it as necessary to fulfil his OSH obligation, the processing of these data might be allowed, as
long as there are appropriate safeguards for the fundamental rights and the interests of the data subject (i.e., the worker)
(Art. 9(4) GDPR).
transparency as to how their algorithms process information and provide recommendations, (2) whether the data on which the AI has been developed are suitable for the specific work and do not repeat previous biases/discrimination, (3) leave some scope for the social partners to adjust the functioning to the work organisation (e.g., in relation to setting targets or the communications of the data collected at work). Moreover, to guarantee and to support the feedback from end users of the AI, reporting mechanisms to third-party agencies should be accessible to workers and their representatives.

These modifications are essential to ensure that the future development and deployment of AI in the work environment will neither lead to worker discrimination, nor represent a threat to workers’ health. It is also fundamental that the implementation of AI at work does not undermine the role of social partners and democracy at work. Currently, the provisions of the AI Act represent a missed opportunity to ensure that AI software being placed on the market is designed in a fair, safe and unbiased manner. To guarantee this, either the AI Act, or a complementary Directive or Regulation, should provide strong counter powers to employer control that workers are presented with in AI systems.

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
The author(s) received no financial support for the research, authorship, and/or publication of this article

ORCID iD
Miriam Kullmann  https://orcid.org/0000-0002-0365-4566