AI Systems for Occupational Safety and Health: From Ethical Concerns to Limited Legal Solutions

Abstract. Digital technologies in the workplace have undergone a remarkable evolution in recent years. Biosensors and wearables that enable data collection and analysis, through artificial intelligence (AI) systems are becoming widespread in the working environment, whether private or public. These systems face strong critics in the media and academia, emphasizing the algorithmic management trend. However, they can also be deployed for the common good such as occupational safety and health (OSH). In this sense, they can be promoted by public authorities in a public policy perspective of OSH, and they can also be used by public employers as a tool to improve the health of workers. Nevertheless, we argue that AI systems for OSH do not exclude thorny problems, considering the sensitive data collected, potential chilling effects, and employment discrimination. Based on three realistic scenarios, we identify a series of ethical concerns raised by the use of such AI systems and elaborate on the legal responses to these issues based on existing European law. With this analysis, we highlight blind spots, that is, situations in which existing laws do not provide clear or satisfying answers to relevant ethical concerns. We conclude that other avenues should be investigated to help the public sector determine whether it is legally and socially acceptable to deploy AI systems and achieve their public policy.

Keywords: Artificial Intelligence, Occupational Health and Safety, Law, Ethics, Public Sector.

1 Introduction

The use of new digital technologies in the workplace has undergone a remarkable evolution in recent years, especially since the outbreak of the Covid crisis [1]. Such development took place in the private and public sector. Artificial intelligence (AI) systems, the internet of things (IoT), advanced robotics, big data applications and mobile devices are among the components of new digital technologies. The high degree of interconnectivity made possible by this digital technology is conductive to what is called 'algorithmic management', when algorithmic software have the power to 'assign, optimize, and evaluate human jobs through algorithms and tracked data' [2, 3]. The increased use of digital technologies has adverse effects repeatedly denounced by media. Specifically, digital intrusion in the workplace becomes an important topic (e.g., Uber monitoring surveillance system [4]; Amazon's AI recruitment tool biased against women [5, 6]). Scholars have highlighted the transformative impact of such technological deployment in the workplace [7, 8]. Digital deployment is also a matter of concern in legal scholarship [9, 10]. The transformative impact of technology in the workplace notably reshape employment relationships, calling into question traditional work cultures related to the place and nature of work, the type of surveillance, and more broadly, the organization and management of the work activities to be performed [11, 12].

Despite these disruptive aspects, new digital technologies may be deployed to favor occupational safety and health (OSH) for workers. If that is the case, positive impacts are to be expected. Examples include the development of protective clothing like smart personal equipment [13, 14]. AI devices may also be deployed for the health or well-being of employees in office jobs. Examples include the deployment of smart watches in the context of corporate wellness programs [15], or emotion-sensing technologies for identifying stressful working situations [16]. However, whenever biosensors connected through AI systems are deployed in the workplace, privacy concerns are raised [17]. Concerns related to surveillance and all sorts of illegitimate pressures on workers and employers need to be taken seriously. They can generate a blurring effect between using technology for OSH purposes and employee evaluations [18].

At the European level, policymakers are aware of the risks related to the increasing deployment of AI and applications in the workplace [19, 20]. In the AI Act proposal, AI systems developed in the context of employment, workers management and access to self-employment are qualified as high-risk AI systems, which have to fulfill new requirements [21, 22]. Another specific legislative proposal – the so-called gig economy directive – especially protects the platform workers [23]. However, in the context of employment, the collection and process of sensitive data for OSH is possible from the perspective of the European General Data Protection (GDPR) law[1]. AI systems for OSH are also not listed as high-risk in the AI act proposal.

Legal constraints related to the deployment of digital technologies may be less important when it clearly serves the purpose of OSH rather than other purposes such as performance management. The reason is that OSH is a public good and should be implemented through a public policy. Nevertheless, we argue that AI systems for OSH do not exclude the thorny dual use issues described above. Facing this risk, rigorous prior analysis should be conducted before the deployment of such technologies.

The aim of this paper is to identify the potential ethical issues raised by the use of digital technologies for the purpose of OSH, to analyze existing legal responses, and to point out where European law fails to address relevant ethical risks. Our analysis contributes to the discussion on the risks and opportunities of the digitalization of work from the perspective of public health promotion. In particular, it informs bodies responsible for public health about the limits of existing regulations in using AI at work.

In this perspective, we begin with background considerations regarding the purpose of OSH and how AI systems can contribute to such a public purpose. Next, we outline the European legal framework. We then elaborate on three realistic scenarios of deployment of IoT for the purpose of OSH and highlight the major ethical issues. In light of these scenarios, we then discuss the possible legal responses to the identified ethical challenges. Thereby, we highlight important blind spots that need to be addressed. We

[1] GDPR, art. 9.2(h).

conclude that it is important to engage the public sector to assess the social and fundamental rights, and setup necessary safeguards before allowing the deployment of an AI system for a public policy purpose.

2 Background

2.1 Maintaining the Safety and Health of Employees

‘Occupational accidents and diseases create a human and economic burden’ [24] and lead to a political response with the recognition of individual workers' rights [25], enshrined in international human rights law[2]. In 1950, the International Labour Organization (ILO) and the World Health Organization (WHO) adopted a common definition of OSH, considering ‘its ultimate goal as the promotion and maintenance of the highest degree of physical, mental and social well-being of workers in all occupations’ [26]. The concept of well-being in occupation was also defined as ‘relate(d) to all aspects of working life, from the quality and safety of the physical environment, the climate at work and work organization’. The measures taken to ensure well-being in the workplace shall then be consistent with those of OSH ‘to make sure workers are safe, healthy, satisfied and engaged at work’. In this perspective, OSH is dealing with the ‘anticipation, recognition, evaluation and control of hazards arising in or from the workplace that could impair the health and well-being of workers, taking into account the possible impact on the surrounding communities and the general environment’ [27].

The protection and promotion of safety and health involves the development of national public policy. To assist States in developing such a policy, the International Labour Organization (ILO) has adopted a series of conventions, recommendations and guides [27].[3] In this perspective, employers have a duty to protect and prevent workers from occupational hazards, but also to inform workers on how to protect their health and that of others, to train their workers, and to compensate them for injuries and illnesses [27]. In the European Union context, based on article 153(2) TFEU, the directive 89/391/EEC of June 12, 1989 addresses measures to encourage improvements in the safety and health of workers at work. Its scope of application concerns the private and public sectors. The employer's obligations are part of a preventive approach [28]. In this respect, States must take measures to ensure that the employer assesses the risks, evaluates those that cannot be avoided, combats them at source, adapts the work to the

[2] Several international texts expressed their commitment for the protection of safety and health of the workers: the 1948 Universal Declaration of Human Rights (art. 23); the 1966 Covenant on Social, Economic and Cultural Rights (art. 7); and the European Social Charter, adopted in 1961 and revised in 1996 (right to safe and healthy working conditions (art. 3), right to health protection (art. 11), obligation to improve work conditions and environment (art. 22).

[3] The ILO Convention, 1981 (No. 155) and its Recommendation (No. 164); the ILO Convention, 1985 (No. 161) and its Recommendation (No. 171); and the ILO Promotional Framework for Occupational Safety and Health Convention (No. 187) and Recommendation (No. 197).

individual, or develops a coherent prevention policy covering technology, working conditions, social relations, and the influence of health-related factors. In addition, when the employer introduces new technologies, they must be subject to consultation with the workers and/or their representatives about the consequences of the choice of equipment, working conditions and environment on the safety and health of the workers. The preventive approach promoted to achieve OSH involves an assessment of the risks that rise in the course of work, which may be related to the use of a new technology.

2.2 AI systems for Occupational Safety and Health

Data-driven health initiatives are gaining interest among employers to improve OSH through monitoring and tracking employees in the workplace [29]. These initiatives rely on the deployment of AI systems that are a combination of software and hardware that enable capturing data and analyzing them to achieve a certain outcome. Among the building blocks of AI systems is the IoT technology. IoT enables access to various types of data in a cyber-physical system. Combined with machine learning algorithms, IoT applications form AI systems that allow the collection and analysis of physical data in the aim of providing actionable insights. With the rapid development of ubiquitous IoT devices, IoT initiatives are being used for self-quantifying and digital monitoring in an aim to detect and prevent health issues and to mitigate health risks [30].

In fact, organizations employ these technologies to collect data related to health, fitness, location and emotions [31, 32]. Wearable technology is most prominently used for such purposes. It includes smart accessories (e.g., smart watches and smart glasses) and smart clothing (e.g., smart shirts and smart shoes) that can record physiological and environmental parameters in real-time, perform analysis to the data, and provide insights to the users in the form of nudges or interventions [33]. Moreover, sensor networks can be placed in different places and are commonly used to detect ambient conditions such as temperature, air quality or occupancy [34, 35]. IoT is used in the workplace for physical health monitoring, either through addressing physical inactivity/sedentary behavior or wrong postures that cause musculoskeletal disorders [36].

In addition, AI systems employing IoT enable emotional health monitoring through detecting occupational stress or burnouts that can affect the health of employees and compromise the quality of work in the long run. This can be achieved through measurement of biomedical data including heart rate and body temperature for estimation of emotional levels most commonly through wearables [37, 38] or facial and speech recognition techniques [39]. These systems allow assessing the employee's state and provide suggestions for healthier habits based on the analyzed data. Moreover, environmental monitoring is another use case for IoT employing sensors (e.g., temperature and humidity) for detecting abnormalities and optimal ambient conditions [40, 41].

The deployment of such technologies in the workplace is then challenging in terms of continuous personal and contextual data collection [42] and its tracking effect [43], information or hidden insights about the employee [44] and the potential bias [46, 47].

3 Legal framework about AI systems in the workplace

The discussion on new technologies has largely focused on the erosion of privacy produced by the indiscriminate processing of data. The current and future technology sophistication goes and will go beyond the question of data privacy. Therefore, the purpose of this section is, on the one hand, to recall the key legal principles in the field of privacy law and, on the other hand, to outline the legislative proposals currently in discussion at the European level that should complement the legal arsenal already in force.

3.1 The Current Legal Framework Regarding Privacy

From the point of view of European human rights and European Union laws, the surveillance inherent in the employment relationship cannot neglect the employees' right to privacy. The European Court of Human Rights ruled that article 8 protects the employee in the performance of his professional duties, thus establishing a limit to the principle of surveillance in employment relationships.[4] It also recognized that between employer and employee's rights, the States have the obligation to balance the interests.[5] If the intrusion is aimed at remedying an employee's behavior that is detrimental to the employer, the intrusion can be justified from the point of view of proportionality.[6] The legal nature of the employer has a consequence on the nature of the obligations of the state.[7] In the case of public organization, the Court ruled that the public actor is directly bound by the conditions for public interference with an individual right, namely the requirement of a legal basis, the public interest and the principle of proportionality.[8]
Moreover, and in accordance with Convention 108+, any personal data processing by public sector authorities should respect the right to private life and comply with the 'three tests' of the principle of proportionality: lawfulness, legitimacy and necessity. The lawfulness test implies checking not only if there is a legal basis but also that such a legal basis is 'sufficiently clear and foreseeable'. It means, for example, that if the rule has a broad content, it will not meet the requirement.[9] In the M.M. case, the Court

[4] ECtHR, Niemietz v. Germany, n°13710/88, 16 December 1992, §§33-34. The Court ruled that 'respect for private life comprised to a certain degree the right to establish and develop relationships with others. There was no reason of principle why the notion of 'private life' should be taken to exclude professional or business activities, since it is in the course of their working lives that the majority of people had a significant opportunity of developing such relationships. To deny the protection of Art. 8 on the ground that the measure complained of related only to professional activities could lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities could not be distinguished'.

[5] ECtHR, Copland v.UK, n°62617/00, 3 April 2007.

[6] ECtHR, Lopez Ribalda and Others v. Spain (GC), n°1874/13 and 8567/13, 17 October 2019, §§ 118, 123.

[7] ECtHR, Bărbulescu v. Romania (GC), n°61496/08, 5 September 2017, §108.

[8] ECtHR, Libert, 22 February 2018, n°588/13; Renfe c. Espagne (déc.), n°35216/97, 8 September 1997 and Copland (mentioned above, §§ 43-44).

[9] ECtHR, Amann v. Switzerland, 16 February 2000, n°22798/95, §76.

indicated that: ‘the greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing to date’.[10] The test of legitimacy implies that personal data undergoing automatic processing must be collected for explicit, specified and legitimate purposes, such as national security, public safety and the economic well-being. The test of necessity includes five requirements: minimization of the amount of data collected; accuracy and updating of data; limiting the data process and storage to what is necessary to fulfil the purpose for which they are recorded, limiting the use of data to the purpose for which they are recorded; and transparency of data processing procedures.

All these requirements for data processing are also enshrined in the GDPR. In the context of employment, the GDPR authorizes member states to specifically regulate the processing of data. The national legislations can cover the ‘recruitment, performance of employment contracts, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment of social benefits in the course of employment or after the termination of the employment relationship’[11]. Nevertheless, member states have to include in their national provisions suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems in the workplace.

The concern with the protection of workers' data also echoes what had already been advocated by the ILO in the context of promoting OSH. Section 14 of Recommendation No. 171 of 1985 provides that OSH services should record data on workers' health in confidential medical files. Persons working in the service should only have access to these records if they are relevant to the performance of their own duties. If the information collected includes personal information covered by medical confidentiality, access should be limited to medical staff. It is also provided that personal data relating to health assessment may only be communicated to third parties with the informed consent of the worker concerned. In 1997, the ILO also adopted a set of practical guidelines on the protection of workers' personal data. In its 2008 position paper, the ILO further recalled that ‘provisions must be adopted to protect the privacy of workers and to ensure that health monitoring is not used for discriminatory purposes or in any other way prejudicial to the interests of workers’ [27].

3.2 The European Legislative Proposals on AI and Algorithmic Management

In addition to the privacy regulation, two European legislative proposals are particularly enlightening in a context of intense technological innovation and the political will to

[10] ECtHR, M.M. v. UK, 13 November 2012, n°24029/07, §200.

[11] See also recital 155.

regulate it while maintaining the balance between the protection of fundamental rights and the economy: the AI act and the Gig economy directive. Both texts address, in their own way and in accordance with the purpose of the regulation, the issue of OSH. In the AI act, safety and health are seen as possible outcomes of AI systems. This type of statement shows that AI systems are seen as potential solutions to the problem of work-related health. In the Gig economy directive proposal[12], the aim is 'ensuring human monitoring of the impact of such automated systems on working conditions with a view to safeguarding basic workers' rights and health and safety at work'[13]. Here, AI systems are not described as a solution, but as potential risk to workers' health. The directive does not intend to prohibit such systems but rather provide a framework for them.

The adoption and implementation of the two texts will complete the European legal framework. For the AI act, its annex III for high-risk AI systems includes those systems that involve 'employment, workers management and access to self-employment', those operating for recruitment purpose and 'contractual relationships, for task allocation and monitoring and evaluating performance and behavior of persons in such relationships'.[14] It is not clear if AI systems for OSH would be concerned. On one side, they are not directly listed, but on the other side, they can be helpful to define the task allocation in the workers management. The gig economy directive proposal will only apply to the digital platform and will not affect other kinds of employment relationships.

Both proposals also make the links with the GDPR. The Gig directive 'provides for more specific rules (for the processing of personal data) in the context of platform work, including to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data within the meaning of Article 88 of Regulation (EU) 2016/679'.[15] Only the explanatory comments of the AI act announced to pursue 'consistency with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality'. The proposal should complement the current legal framework with 'a set of harmonized rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems'. Furthermore, the AI Act proposal complements existing Union law on non-discrimination with specific requirements that aim to minimize the risk of algorithmic discrimination, in relation to the design and the quality of datasets used within the AI systems.

4 Ethical Considerations of AI Systems for OSH

In order to identify concerns associated with the implementation of AI technology in the workplace, we have developed three realistic scenarios involving the deployment

[12] European Commission, Proposal for Directive of the European Parliament and of the Council on improving working conditions in platform work, 2021/0414(COD).

[13] *Ibidem.*

[14] Annex III ; recital 36.

[15] Recital 29, Gig economy directive.

on the workplace of technological solutions currently available on the market. These three scenarios were presented and discussed in a workshop hosted in December 2021 with ten stakeholders of various expertise in technology, medicine, politics, and ethics. All stakeholders evaluated the scenarios as highly plausible. Based on the workshop discussion[16] and on ethical principles identified in the 2019 report on AI trustworthiness of the independent high level expert group on AI set up by the European Commission (AI HLEG) [20], we highlight a series of ethical concerns raised by the deployment of new technologies for OSH purposes.

4.1 Scenarios

In the three presented scenarios, the purpose of the technology implementation is promoting the health of the employees and ameliorating their working conditions. Each scenario describes a different context of implementation of a different device or technology that collects employee's health-relevant data and outputs reports. The scenarios vary with respect to what type of health data are collected (posture on a chair, step count, voice tone, etc.) how the device is proposed to employees (consultation, information, opt-out options), how the data is managed (e.g., sent to external companies or not) and processed (e.g., results anonymized or not), and who received the report (employees, occupational physician, human resource).

Scenario 1: Smart chairs for monitoring sedentary behavior
The first scenario discusses the use of smart chairs to avoid chronic illnesses resulting from employees' posture while working. These smart chairs detect wrong posture for neck, head and back movements and a red light switches on whenever its user takes a wrong posture over several minutes. They also produce a light sound as a nudge to inform users when they were seated for a too long period of time. The smart chairs are delivered with a program that stores data about users' posture and sitting time and generates individual reports including health advice.

Scenario 2: Steps contest in a corporate wellness program
The second scenario discusses the organization of steps contest within a corporate wellness program that aims to motivate employees to engage in more physical activity for the benefit of their health. Employees' steps are monitored by smartwatches provided by the company to all employees willing to participate. The smartwatches monitor users' steps, speed of motion, heart rate, body temperature, and blood pressure. On a comprehensive app user interface, participants can access personalized reports of users' step performance, general activity, and global physical health.

[16] In addition to the workshop, we conducted a series of individual interviews with a diversified panel of stakeholders. A qualitative analysis of these data will be published in a separate paper.

Scenario 3: Stress monitoring and management
The third scenario discusses the use of sensors network in order to assess employees' satisfaction with the flexible work policy and stress level related to their working conditions and workload. Computers used by the employees are equipped with sensors capturing speech tone and speed (disregarding content). Information collected by the sensors are processed by deep learning algorithms, which output an assessment of individual stress level and emotional state. These algorithms produce real-time signals and recommendations to employees (such as "It may be the right moment for a break"). Also, reports of overall stress levels are sent periodically to the employees who are encouraged to share them with their direct supervisors as a basis for discussing their satisfaction with the working conditions and workload.

4.2 Ethical Considerations

Our first general concern is the question of trust: trust in the technology and its intended use, trust in the employer and its actual use. A linked topic is the question of ensuring that the technology is the right answer to the right problem. For instance, is the smart chair an appropriate response to employees' back pain or shouldn't other organizational changes (working schedule, changes of working tasks) be made to meet the same aim more efficiently? Additionally, what is the real employer's intention in deploying such a technology? Indeed, despite the fact that the three scenarios represent cases of monitoring for health improvement due to the technologies used and the type of data collected, it cannot be excluded that these tools can be used for other purposes. Moreover, the deployed systems are equipped with a nudging mechanism. Is such an incentive to behave in a certain way likely to have negative consequences for the worker if they choose not to comply with it? For example, in the scenario of the smart chair case, can employees be held responsible for health problems they could have avoided (e.g., back pain)? Could they be deprived of social protection? These elements thus mainly reflect the requirement of fairness and, secondarily, that of preventing (indirect) harm.

The issue of employee's choice and employer power is also raised in all three scenarios. In fact, even if consent is required for using the technology or for participating in a fitness contest, the consent could be ill-founded in a company environment because there are doubts about the degree of free of choice of the worker. Indeed, if there is a management decision, employees may feel the need to follow it to avoid any discrimination or punishment resulting from not participating or opposing the use of the new system. In addition, financial incentives may influence employees' judgment (e.g., the provision of smartwatches in the second scenario), which may be seen as a form of indirect pressure to participate since a reward is involved, thus intensifying the power imbalance within the organization. All these elements raise the issue of respecting the employee's autonomy in the employment relationship.

Another important concern is the risk of discrimination. This is mainly associated with the use of special devices and algorithmic decision-making. In fact, the main question is how to guarantee the accuracy of the devices in collecting the data and the algorithmic correctness. If the data is biased or the algorithm is biased, we might result with discrimination based on progressive error from the AI system. Moreover, data collected by the IoT devices correspond to health information, location and behavior. This can be analyzed to assess the working capacities and capabilities of the employees and can result with discrimination act if used in the long-term; for instance, to hire or promote employees with good potential based on the analysis and terminate contracts for employees who show lower performance results in terms of work and health. Here again, these issues echoed the principles of fairness and prevention of harm.

Privacy is also a central concern when it comes to collecting and processing personal data. In the three scenarios, the employer owns the systems used in the workplace, but data generated is managed and processed by third parties in most cases. Thus, the worker has no or limited control over the data collection, use and sharing, which creates a problem of privacy. This concern is particularly significant with medical data collection. With extensive data collection, the privacy risk increases as the data processing can reveal information about the employee's health.

Another issue is employer surveillance. This is also connected to the intended purpose of use for the system deployed. As mentioned earlier, the technology is being used for health monitoring, but other forms of monitoring related to work performance can result with erasure of individuality. In this sense, the technology can create a chilling effect, a sort of behavior shaping. When a worker knows that he is monitored, they might change their behavior and working methods will be shaped for social conformity. Another issue with such technologies is related to the surveillance at home. The current situation with flexible work policy and remote working creates more challenges. This is especially the case for scenario two that requires the use of a wearable device for health monitoring. In this scenario, the smart watches can be used by workers all day and the data collected correspond to their physical activity and health status at work and in their private life. The third scenario also strengthen this concern, where in a remote working setting interactions in the surrounding are being monitored, not only related to the work context which is also one type of surveillance that trespasses the privacy of others (i.e., extrinsic privacy). All these elements regarding privacy and employer surveillance further underline the principles of prevention of harm and fairness.

5 Legal Analysis

In order to move from the inductive and heuristic approach previously followed to the deductive and interpretative approach adopted in legal doctrine, we applied the judicial reasoning of subsumption, which makes it possible to move from facts to legal rules. In this process, their connection to ethical principles makes it possible to identify whether legal rules can answer them. Given that AI systems for OSH lie at the intersection of several legal areas, we limit our legal analysis to the key norms concerning the Fundamental Rights Act, the OSH Directive, the GDPR and the proposed Regulation on AI. The Gig economy proposal will complement this legal analysis in that it identifies avenues of protection for all employees. Moreover, given the technological development, the law does not always offer a legal answer to new problems. A legal interpretation *de lege lata* will be proposed for those that remain unanswered.

The *trust* concerns, which was mainly related to fairness, can be analyzed in the light of the legal legitimacy principle. This principle is part of the classic proportionality test involving determining whether the means is adequate to achieve the desired end. It is also one of the fundamental principles that the states must respect in its action. In the case of a public employer, who is also bound to respect the fundamental rights of its employees, it means that the employer will have to verify that the digital device has established effectiveness regarding the public health problem. The legitimacy principle is also useful to address the purpose and repurposing concerns. Those are related to an unintended use of the device, which could by ricochet violate the data purpose principle of the GDPR. [17] The respect of the purposed intended use of the device is also expressed in the proposal of AI act.[18]

The *trust* concerns can also be addressed with the right of information. This is a fundamental right for workers as well. The OSH directive provides under its article 12, a general obligation to the employer for ensuring 'information and instructions (…) in the event of introduction of any new technology'.[19] The directive also provides that the employer inform and consult employees and/or their representants[20]. From the GDPR perspective, such a right is also guaranteed to the data subject. Any data process shall be operated in respect of the transparency principle.[21] The AI act should impose to complement different types of information that will reinforce this information principle.[22] In this case, such obligation of information will be limited to the AI providers and in the case of high-risks AI systems, in which systems for OSH do not seem enlisted. The digital economy directive will go one step further. Digital labour platforms will have to inform platform workers, especially when the AI system can influence their OSH.[23] This can be understood as an extra level of information, emphasizing that workers should be informed about any digital device, including an automated monitoring and decision-making systems to promote workers' health.

The *autonomy concerns* can be analyzed in the light of three legal norms and principles: article 8 ECHR, the consent requirement regarding data processing and the principle of

[17] Art. 6 GDPR concerning the lawfulness of the processing; See also art. 9 GDPR concerning the processing of special categories of personal data such as health data; See art. 88 in the context of processing in the context of employment; See recital 50 of the GPDR on the initial link between the purposes for which the data have been collected and the purposes of the intended further processing.

[18] The intended purpose principle, as defined in art.3(12), is mentioned 37 in the AI Act and is at the core of the regulation. Requirements (recital (43) and assessment of the risks are assessed at the light of the intended purpose of the system (Recital (42)) and new conformity assessment occurs when the intended purpose of the system changes (recital 66).

[19] Art. 12. 1 OSH Directive

[20] Art. 6.3 (c) OSHA directive; such obligation is recalled in the Gig economy directive proposal (art. 6, see also detailed explanation of art. 6, p. 16).

[21] Art. 12 GDPR.

[22] Art. 13.3 AI Act

[23] Art. 12 GDPR, Art. 6 Gig Economy Directive; recital 32 Gig Economy.

non-discrimination. Considering that technology has a social and individual impact, the digital device could be analyzed as limiting its autonomy. In such a case, the public employer shall respect the principle of proportionality and proceed to the three tests of lawfulness, legitimacy, and necessity.

From the point of view of the GDPR, the autonomy concern can also be related to the consent requirement. On this point, both the European data protection authority and legal scholars [48, 49] agree that, in the working environment, consent could not be considered free and informed. For this, a legal basis for the processing of data is necessary. The field of OSH is precisely a legitimate purpose.[24] Moreover, employees have the right not to be subject to automated individual decision-making, but such right is related to the risk that such decision significantly affects the circumstances, behavior or choices of the individuals concerned (WP art. 29, opinion on automated decision).[25] If we take into account recital 32 of the Gig economy directive proposal, which states that the impacts on health fall into this category of effects justifying opposition to an automatic decision and established the link with psychosocial problems, then we can argue that employees may object to the fact that these connected objects for health purposes may allow a reorganization of their work.

The autonomy issues can finally be addressed in light of the principle of non-discrimination. On this point, the discrimination risk appears at two levels: in the dataset and through the outcomes of the device. Regarding the dataset, it emphasizes a question of data quality (relevance, representativity, completeness and freedom of errors). The AI Act directly addresses the question of bias in the dataset. Still, it is only an obligation for the providers who have to process special categories of data such as health data or biometric data in the way that ensuring the detection, correction and erasure of bias in notably high-risk AI systems[26]. Nevertheless, users of AI systems such as public sector actors are obliged to respect the principle of equality between individuals. There is therefore a problem here in determining the level of responsibility. Moreover, the discrimination risk is on the outcomes of the devices, also echoed to the problem of chilling effect. It happens when 'people might feel inclined to adapt their behavior to a certain norm'. Technology is likely to lead individuals to change their behavior without them even being aware of it. In this perspective, technology can be viewed as problematic regarding the right to individual self-determination.[27]

The last concern is employee *privacy,* which was related to the blurring effect between professional and personal life. This ethical problem is directly addressed under the right to private life, the right to protection of personal data, the convention 108+ and the

[24] Art. 9. 2 (h) GDPR; art. 6 OSH directive.

[25] Art. 22. 1 GDPR.

[26] Recital 44 AI Act.

[27] It must be added here that the Gig economy proposal indicates that 'such systems may perpetuate historical patterns of discrimination' towards particular groups such as woman, certain age groups'. The European Commission could complement existing Union law on discrimination with specific requirements for minimizing the risk of algorithmic discrimination (See detailed explanation of consistency with existing policy provisions in the policy area p.4).

GDPR. Here, we can add that the employer has to minimize the data collection, limiting it to health' purpose, and finally destroy such data. However, compliance with the minimization and purpose requirement may be particularly challenging to achieve if the device cannot discriminate between data produced by other users - for example, family members - who would also have access to these tools within the family. Moreover, companies that continue to play a role in data analysis develop a substantial proportion of these technological tools. In such a situation, the public employer must also respect its obligations towards this party. Finally, if the digital device targets the recognition of micro-expressions, voice tone, heart rate, and temperature to assess or even predict our behavior, mental state and emotions, it must be considered as an intrusive tool that collects biometric data.[28] Here again, there is a legal gap. As mentioned by the 2020 CAHAI report, biometric data used for another aim than recognition, such as categorization (for example, for the purpose of determining insurance premium based on statistical prevalence health problems), profiling, or assessing person's behavior, might not fall under the GDPR definition.

This short legal assessment of the ethical issues shows that the law does not offer an answer to all the problems identified by stakeholders. Nevertheless, it is worth noting that the components of the principle of proportionality appear several times and make it possible to recall the importance of this legal principle in the case of reflection on the deployment of technology. This evaluation also showed the points of discussion that still need to be pursued concerning the deployment of AI systems, especially from the point of view of respect for individual autonomy and infringements of personal data.

6 Conclusion: Proposal for Social and Human Rights Assessment

This paper discusses the deployment of AI systems for OSH in the public sector. In this context, we argued that the deployment of such systems for OSH has a good purpose, which does not exclude thorny issues. From this perspective, the issues may be legal and ethical. Indeed, AI systems are not deployed in a legal vacuum. They have to meet initial requirements. However, they may generate problems that are sometimes not directly identifiable or have not been taken into account from a legal point of view. To map these problems, the inductive approach followed in this paper allowed us to identify ethical concerns regarding the implementation of AI systems for OSH, this enabled us to examine whether the law imposes duties and rights in such situations. From this perspective, we show that the legal answers were sometimes insufficient, leaving room for maneuver for the user of the AI system. Therefore, such a conclusion forces us to ask whether the law should not be strengthened here.

Other avenues should still be explored considering the AI systems' rapid deployment. Indeed, from a practical point of view, one may wonder whether the logic of subsumption followed in the sections 4 and 5 is not the most logical way to assess the relevance

[28] The CAHAI report underlines that there is no sound scientific evidence corroborating that a person's inner emotions or mental state can be accurately 'read' from a person's face, heart rate, tone or temperature.

to deploy an IA system, rather than thinking *in asbtracto* from legal rules and principles and then from ethical values. To address that, in [50, 51], the authors call for impact assessment, and in [52] developed tests for fairness automation. In the framework of the public sector, all these proposals should also be examined in the light of the recommendations on better regulation, considering AI systems as tools for implementing public policy. While the data protection impact assessment, imposed by the GDPR, is one tool to assess the privacy risks for data processing technologies (including AI systems), we believe that such an impact assessment should not be limited to a consequentialist approach to the problem. We suggest a more inclusive approach to the assessment to comprise a social and huma rights impact assessment with stakeholders that should focus on identifying ethical concerns and respecting public values.

References

1. Samek Lodovici et al.: Teleworking and digital work on workers and society. Special focus on survaillance and monitoring, as well as on mental health of workers. European Parliament (2021)
2. Lee, M.K., Kusbit, D., Metsky, E., Dabbish, L.: Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers (2015)
3. Kaoosji, S.: Worker and Community Organizing to Challenge Amazon's Algorithmic Threat. In: Alimahomed-Wilson, Ellen, J.R. (eds.) The Cost of Free Shipping, pp. 194-206. Pluto Press (2020)
4. de Chant, T.: Uber asked contractor to allow video surveillance in employee homes, bedrooms : Employee contract lets company install video cameras in personal spaces. Ars technica, (2021)
5. Dastin, T.: Amazon scraps secret AI recruiting tool that showed bias against women. Reuters, (2018)
6. Manokha, I.: New Means of Workplace Surveillance. Monthly Review, vol. 70, (2019)
7. Ajunwa, I., Crawford, K., Schultz, J.: Limitless Worker Surveillance. California Law Review 105, 735-776 (2017)
8. Moore, P., Piwek, L.: Regulating wellbeing in the brave new quantified workplace. Employee Relations 39, 308-316 (2017)
9. Aloisi, A., Gramano, E.: Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context. Special Issue of Comparative Labor Law & Policy Journal 41, 95-122 (2019)
10. Hendrickx, F.: From Digits to Robots: The Privacy-Autonomy Nexus in New Labor Law Machinery. Comparative Labor Law & Policy Journal 365-388 (2019)
11. Aloisi, A., De Stefano, V.: Essential jobs, remote work and digital surveillance: addressing the COVID-19 pandemic panopticon. International Labor Review (2022)
12. Aloisi, A., Gramano, E.: Artificial intelligence is watching you at work: digital surveillance, employee monitoring, and regulatory issues in the EU Context. Comp. Lab. L. & Pol'y J. 41, 95 (2019)
13. Thierbach, M.: Smart personal protective equipment: intelligent protection for the future. European Agency for Safety and Health at Work (2020)
14. Kim, S., Moore, A., Srinivasan, D., Akanmu, A., Barr, A., Harris-Adamson, C., Rempel, D.M., Nussbaum, M.A.: Potential of Exoskeleton Technologies to Enhance Safety, Health, and Performance in Construction: Industry Perspectives and Future Research Directions. IISE Transactions on Occupational Ergonomics and Human Factors 7, 185-191 (2019)

15. Burke, R., Richardsen, A.e.: Corporate Wellness Programs: Linking Employee and Organizational Health (2014)
16. Whelan, E., McDuff, D., Gleasure, R., vom Brocke, J.: How Emotion-Sensing Technology can Reshape the Workplace. MITSloan Management Review (2018)
17. Collins, P.M., Marassi, S.: Is That Lawful?: Data Privacy and Fitness Trackers in the Workplace. International Journal of Comparative Labour Law 37, 65-94 (2021)
18. Akhtar, P., Moore, P.: The Psychosocial Impacts of Technological Change in Contemporary Workplaces, and Trade Union Responses. International Journal of Labour Research 8, 101-131 (2016)
19. CAHAI - Ad hoc Committee on Artificial Intelligence: Towards a Regulation of AI Systems: Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law. Ad Hoc Committee on Artificial Intelligence, Council of Europe (2020)
20. Independent High-Level Expert Group on Artificial Intelligence: Ethics guidelines for trustworthy AI, Publications Office, 2019. European Commission (2019)
21. Vaele, M., Zuiderveen Borgesius, F.: Demystifying the Draft EU Artificial Intelligence Act Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International (2021)
22. Ebers, M., Hoch, V.R.S., Rosenkranz, F., Ruschemeier, H., Steinrötter, B.: The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). Multidisciplinary Scientific Journal 4, 589–603 (2021)
23. Tan, Z.M., Aggarwal, N., Cowls, J., Morley, J., Taddeo, M., Floridi, L.: The ethical debate about the gig economy: A review and critical analysis. Technology in Society 65, 101594 (2021)
24. ILO: Builidinf a preventive safety and health culture. A guide to the Occupational Safety and Health Convention, 1981 (n°155), its guide Protocole and the Promotional Framework for Occupational Safety and Health Convention, 2006 (n°187). (2013)
25. Abrams, H.K.: A Short History of Occupational Health. Journal of Public Health Policy 22, 34-80 (2001)
26. Organisation, I.L.: ILO standards-related activities in the area of occupational safety and health: An in-depth study for discussion with a view to the elaboration of a plan of action for such activities. In: Office, L. (ed.), Geneva (2003)
27. Alli, B.O.: Fundamental principles of occupational health and safety (2008)
28. Raworth, P.: Regional Harmonization of Occupational Health Rules: The European Example. American Journal of Law & Medecine 21, 7-44 (1995)
29. Charitsis, V.: Survival of the (data) fit: Self-surveillance, corporate wellness, and the platformization of healthcare. Surveillance & Society 17, 139-144 (2019)
30. Yassaee, M., Mettler, T., Winter, R.: Principles for the design of digital occupational health systems. Elsevier (2019)
31. Manokha, I.: The Implications of Digital Employee Monitoring and People Analytics for Power Relations in the Workplace. Surveillance & Society 18, 540-554 (2020)
32. Giddens, L., Leidner, D., Gonzalez, E.: The role of Fitbits in corporate wellness programs: Does step count matter? Proceedings of the 2017 Hawaii International Conference on System Sciences pp. 3627-3635, Hawaii (2017)
33. Fdez-Arroyabe, P., Fernández, D.S., Andrés, J.B.: Chapter 6 - Work Environment and Healthcare: a Biometeorological Approach based on Wearables. In: Dey, N., Ashour, A.S., James Fong, S., Bhatt, C. (eds.) Wearable and Implantable Medical Devices, vol. 7, pp. 141-161. Academic Press (2020)
34. Afolaranmi, S.O., Ramis Ferrer, B., Martinez Lastra, J.L.: Technology Review: Prototyping Platforms for Monitoring Ambient Conditions. International Journal of Environmental Health Research 28, 253-279 (2018)

35. Saini, J., Dutta, M., Marques, G.: A Comprehensive Review on Indoor Air Quality Monitoring Systems for Enhanced Public Health. Sustainable Environment Research 30, 6 (2020)
36. Gorm, N., Shklovski, I.: Sharing Steps in the Workplace: Changing Privacy Concerns over Time. In: Proceedings of the 2016 CHI conference on human factors in computing systems, pp. 4315-4319. (Year)
37. Han, L., Zhang, Q., Chen, X., Zhan, Q., Yang, T., Zhao, Z.: Detecting work-related stress with a wearable device. Computers in Industry 90, 42-49 (2017)
38. Stepanovic, S., Mozgovoy, V., Mettler, T.: Designing Visualizations for Workplace Stress Management: Results of a Pilot Study at a Swiss Municipality. In: Proceedings of the International Conference on Electronic Government, pp. 94-104. Springer, (Year)
39. Fugini, M., Barenghi, A., Comai, S., Pelosi, G., Tedesco, R., van Gasteren, M., Catalina, C.A., Arribas Leal, E., Losada Durán, R., Martins de Almeida, R.M.: WorkingAge: Providing Occupational Safety through Pervasive Sensing and Data Driven Behavior Modeling. In: Proceedings of the 30th European Safety and Reliability Conference, pp. 1-8. (Year)
40. Nižetić, S., Pivac, N., Zanki, V., Papadopoulos, A.M.: Application of Smart Wearable Sensors in Office Buildings for Modelling of Occupants' Metabolic Responses. Energy and Buildings 226, 110399 (2020)
41. van der Valk, S., Myers, T., Atkinson, I., Mohring, K.: Sensor Networks in Workplaces: Correlating Comfort and Productivity. In: Proceedings of the 10th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp. 1-6. IEEE, (Year)
42. Souza, M., Miyagawa, T., Melo, P., Maciel, F.: Wellness programs: Wearable technologies supporting healthy habits and corporate costs reduction. Proceedings of the 2017 International Conference on Human-Computer Interaction, pp. 293-300. Springer, Vancouver, Canada (2017)
43. Hall, K., Oesterle, S., Watkowski, L., Liebel, S.: A Literature Review on the Risks and Potentials of Tracking and Monitoring eHealth Technologies in the Context of Occupational Health Management. (2022)
44. Gaur, B., Shukla, V.K., Verma, A.: Strengthening people analytics through wearable IOT device for real-time data collection. Proceedings of the 2019 International Conference on Automation, Computational and Technology Management, pp. 555-560. IEEE, London, UK (2019)
45. Feuerriegel, S., Dolata, M., Schwabe, G.: Fair AI: Challenges and opportunities. Business & Information Systems Engineering 62, 379-384 (2020)
46. Siau, K., Wang, W.: Building trust in artificial intelligence, machine learning, and robotics. Cutter business technology journal 31, 47-53 (2018)
47. Feuerriegel, S., Dolata, M., Schwabe, G.: Fair AI. Business & information systems engineering 62, 379-384 (2020)
48. WP29: Opinion 2/2017 on data processing at work. In: Party, A.D.P.W. (ed.), (2017)
49. Brassart Olsen, C.: To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR. International Data Privacy Law 10, 236-252 (2020)
50. Jasanoff, S.: The ethics of invention : technology and the human future. WW. Norton & Company (2016)
51. Metcalf, J., Moss, E., Watkins, E., Singh, R., Elish, M.C.: Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts ACM Conference on Fairness, Accountability,and Transparency (FAccT '21), Canada.ACM (2021)
52. Wachter, S., Mittelstadt, B., Russell, C.: Why Fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. Computer Law & Security Review 41, 72 (2021)