Hoffmann, Mia; Mariniello, Mario

Research Report

Biometric technologies at work: A proposed use-based taxonomy

Bruegel Policy Contribution, No. 23/2021

Provided in Cooperation with:
Bruegel, Brussels

Suggested Citation: Hoffmann, Mia; Mariniello, Mario (2021) : Biometric technologies at work: A proposed use-based taxonomy, Bruegel Policy Contribution, No. 23/2021, Bruegel, Brussels

This Version is available at:
https://hdl.handle.net/10419/270503

Policy Contribution
Issue n°23/21 | November 2021

Biometric technologies at work: a proposed use-based taxonomy

Mia Hoffmann, Mario Mariniello

Executive summary

BIOMETRIC TECHNOLOGIES HAVE in principle the potential to significantly improve worker productivity, security and safety. However, they are also a source of new risks, including exposure to potential personal data abuse or the psychological distress caused by permanent monitoring. The European Union lacks a coherent regulatory framework on the mitigation of risks arising from the use of biometric technologies in the workplace.

WE PROPOSE A taxonomy to underpin the use of artificial intelligence-powered biometric technologies in the workplace. Technologies can be classified into four broad categories based on their main function: (1) security, (2) recruitment, (3) monitoring, (4) safety and well-being. We identify the benefits and risks linked to each category.

TO BE MORE effective, EU regulation of artificial intelligence (AI) in the workplace should integrate more detail on technology use. It should also address the current scarcity of granular data by sourcing information from users of AI technologies, not only providers.

THERE IS AN untapped potential for technology to address workplace health hazards. Policymakers should design incentive mechanisms to encourage adoption of the technologies with the greatest potential to benefit workers.

ARTIFICIAL INTELLIGENCE USERS, in particular bigger companies, should be required to assess the effect of AI adoption on work processes, with the active participation of their workforces.

MIA HOFFMANN (mia.hoffmann@bruegel.org) is a Research Assistant at Bruegel

MARIO MARINIELLO (mario.mariniello@bruegel.org) is a Senior Fellow at Bruegel

This Policy Contribution was produced within the project 'Future of Work and Inclusive Growth in Europe', with the financial support of the Mastercard Center for Inclusive Growth

Recommended citation
Hoffmann, M. and M. Mariniello (2021) 'Biometric technologies at work: a proposed use-based taxonomy', *Policy Contribution* 23/2021, Bruegel

1 Introduction

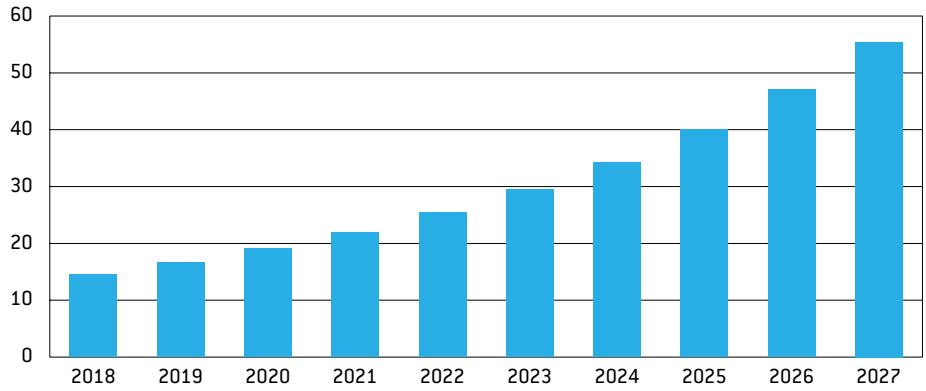
Traditionally, the analysis of the impact of technology on labour markets has focused on measurement of the quantitative effects on aggregate employment. Researchers often ask whether technology will create more jobs than it will destroy, or which jobs are more exposed to the risk of disappearing because machines will replace humans. But a parallel question is becoming increasingly pressing. Technology may not have a significant negative impact on the quantity of jobs available to humans, but it certainly transforms them, changing how jobs are performed, with implications for workers' quality of life and for productivity. Hence the focus shifts from a quantitative to a qualitative perspective.

Addressing this has become even more pressing in the wake of the COVID-19 pandemic, which has pushed companies to increase their adoption of digital technologies, with varying impacts on the wellbeing of workers (for example, during the pandemic investment by employers in monitoring and surveillance software has increased significantly; see Kropp, 2021; Mascellino, 2020). Meanwhile, the disruptive potential of the pandemic has provided employers with an opportunity to introduce new work processes and redesign workplaces to address long-standing issues, such as workplace health hazards, that technology can help deal with.

We focus on artificial intelligence (AI)-powered biometric technology used in the workplace. Biometrics refers to the automated recognition of a person based on their physical and behavioural characteristics (Sabhanayagam *et al*, 2018; Sundararajan and Woodard, 2018). Identity recognition includes identification ('*Who are you?*') and verification ('*Are you really who you say you are?*'). But the use of AI-powered biometric technologies in the workplace can go well beyond recognising identity. For the purposes of this Policy Contribution we define biometric technologies as AI technologies that rely on biometric data to derive inferences about the individual whose data is collected. Such inference can include individuals' moods, their level of concentration, their health or personality. Even when the purpose of such soft biometrics is not to identify individuals, their deployment still has far-reaching implications for workers and workplaces, not least with respect to privacy (McStay, 2020).

The global biometrics market is growing fast. Estimates from 2019 expected global revenues to almost double within the next four years, and reach $55.42 billion in 2027 (Figure 1). This data includes the use of biometrics across all domains, including law enforcement and in customer-centric applications.

Figure 1: Global biometric technology market revenue in $ billions, 2018-2027



Source: Bruegel based on Statista, https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue. Note: Values from 2020 on are forecasts.

Comprehensive data on the use of biometric technology in workplaces is scarce, a problem that should be addressed by policymakers. Because the adoption of new technologies in the workplace has significant potential to affect workers' well-being, a first key step is to improve the ability of public authorities to accurately monitor this phenomenon as it unfolds. According to one survey (European Commission, 2020), 42 percent of enterprises in the EU use at least one kind of AI technology, but information is lacking about whether the AI technologies are applied to employees or customers, and no distinction is made between biometric and non-biometric systems[1]. Analysis in European Commission (2020) by individual technology shows that those that can be classified as biometric technologies are among the less-utilised: natural-language processing (speech recognition, machine translation or chatbots) has been adopted by only one in ten firms, while 9 percent of enterprises use computer vision (visual diagnostics, face or image recognition), and the use of sentiment analysis (analysis of emotion and behaviour) is even rarer, at 3 percent[2]. A few sectors, including social work, education and real estate predominantly adopt AI systems related to biometrics, but overall adoption levels are very low. Skill shortages, both in the labour market and internally, represent major obstacles to the adoption of AI technologies in general. However, for the adoption of sentiment analysis, reputational risks and lack of citizen's trust represent significant adoption barriers. These barriers are not considered very problematic for other technologies.

The increasing interest of regulatory authority in these markets is therefore not coincidental. The European Union, for example, has been increasingly active in recent years in attempting to define a legal framework to mitigate the risks of abuse arising from advanced technology. The general data protection regulation (GDPR), which entered into force in 2018, is the bluntest example. In April 2021, the European Commission proposed harmonised rules on artificial intelligence, commonly referred to as the 'AI Act' proposal (European Commission, 2021a). The main goals of the proposed AI Act are to create the conditions for ethical AI and the concrete enforcement of rules that mitigate AI risk, especially as experienced by the most vulnerable. For the workplace, the proposed AI Act specifically lists as high-risk:

- *"AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;*
- *"AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior* [sic] *of persons in such relationships"* (European Commission, 2021a).

The proposed AI Act, however, does not provide details about the identified sources of risk when artificial intelligence is used in the workplace. Nor does it explain through which mechanisms risk can arguably translate into harm for workers. However, such explanations are needed to disentangle potentially harmful from potentially beneficial use of technology. Furthermore, the proposed AI Act would impose a number of requirements for providers and users of high-risk AI applications. These include risk management and assessment of potential current and future risks. However, no specific guidelines are given on how that assessment should be done (for example, what should be considered a 'foreseeable risk' associated with the use of biometric technology in the workplace?).

We aim to fill the gap in the proposed AI Act by classifying technologies and explaining

1 European Commission (2020) is a survey of firms that provides useful general insights but does not enable conclusions to be drawn about specific use cases.

2 European Commission (2020), while aiming for representativeness, suffers from a low response rate of only 5 percent on average, which likely biases the adoption rate upwards. Therefore, the accuracy of the exact adoption rates may be limited. We believe, nonetheless, that in the absence of more reliable estimates the relative scarcity of biometric technologies compared to other technologies considered, is a realistic assessment.

how technology in the workplace can harm workers. To our knowledge, this is the first attempt to propose a taxonomy of biometric technologies used in the workplace[3]. Our analysis furthermore suggests improvements that could be made to the AI Act draft text. In particular, the text should include a bigger emphasis on the role played by users of AI applications. As drafted by the European Commission, the proposed AI Act does not entail sourcing data on high-risk applications directly from, for example, companies that adopt them. However, lack of granular use data can significantly hamper regulators' ability to understand how harm to workers can unfold at plant level. Moreover, the AI Act is geared to compelling providers of high-risk AI applications to improve their products. However, AI applications may have significant redistributive effects when they are adopted, depending on the environment in which they are used. Such risks may not be entirely foreseeable by AI providers. It would thus be desirable that users should also engage in strategies that mitigate potential risks. In particular, bigger companies could be required to assess the effects of high-risk AI applications on their workforces, with workers actively participating in such assessments.

2 Biometric technologies at work: a proposed use-based taxonomy

Biometric technologies can be categorised into three groups:

- Physical;
- Physiological;
- Behavioural.

Physical biometrics refers to data on static and unique bodily characteristics. Examples include DNA, fingerprints, iris and retina patterns and physiognomy, but thanks to technological progress, options now extend to include ear, palm and vein patterns and many more. Raw biometric data is collected through a live scan or a digital image, which is then processed and translated into unique code. In facial recognition, for instance, this code reflects the size of the mouth, position and shape of the nose, the distance between the eyes, and so on (Sabhanayagam *et al*, 2018).

Physiological biometrics is data on a person's physiological functioning, such as their heart rate, blood pressure, oxygen level and muscle use. While monitoring of this data is common in healthcare, physiological biometrics are increasingly moving into workplaces, especially for workplace health assessment (Mettler and Wulf, 2019).

Behavioural biometrics use patterns of human behaviour as the basis for analysis and are driven by deep-learning techniques. The underlying concept of the technology is to exploit distinct patterns of human behaviour as a means for authentication and identification, either in real-time or retrospectively (Liang *et al*, 2020). Behavioural biometrics extract information not from the outcome of an action, but from the way it is executed. For example, identity is verified by a worker's gait, while mood is evaluated from the pitch of their voice. A benefit is that data is collected without interrupting individuals in their ongoing activity in a way that an ID check or employee survey would. The ubiquity of smart devices, cameras and sensors contributes to the technology's growing importance in workplaces.

Regardless of the type of biometric technology, data analysis follows a similar, automated process. Raw biometric data is collected via sensors, cameras, microphones or other devices

3 An extended version of the taxonomy with more detail is available in Hoffmann and Mariniello (2022).

and pre-processed to remove noise and clean the data. This is followed by feature extraction. Features are specific biometric data points or patterns considered to be indicative or predictive of the outcome of interest. For example, for identification, one of the features could be the distance between the eyes, or the pressure applied on certain keys while typing. It could be the percentage of speaking time to assess personality, and the breathing rhythm to judge stress levels (Han *et al*, 2017; Liang *et al*, 2020; Sabhanayagam *et al*, 2018; Vinciarelli and Mohammadi, 2014). Depending on the type and amount of raw data, this step requires more or less computing power. Depending on the use case, the extracted features are fed into diverse AI models that determine the outcome of interest (such as classification, authentication or identification).

Biometric AI systems can serve a wide range of functions in the workplace. Providing security by verifying and identifying workers is one, but as we will illustrate in the next sections, there are many other purposes, including those relying on physiological and behavioural biometric data. An important emerging field in this regard is affective computing (Yanushkevich *et al*, 2020). This refers to the computational analysis of data on human behaviour, such as facial expressions, gestures and language, or physiology, for its emotional information to derive conclusions about a person's affective state, including emotions (Balan *et al*, 2020; Richardson, 2020), mood (Zenonos *et al*, 2016), personality (Mehta *et al*, 2020; Vinciarelli and Mohammadi, 2014) or stress levels (Khowaja *et al*, 2021). The analysis builds on several biometric technologies including facial expression recognition, tone analysis and natural language processing, and is typically based on the assumption that there are common and universal forms of emotional expression regardless of culture, gender, age or race (Barrett *et al*, 2019; Richardson, 2020).

Table 1: A taxonomy for biometric AI systems in the workplace

Purpose	Technologies used	Use case	Real life example/brand
Security	Facial, fingerprint, gait, keystroke recognition	Access control, continuous authentication	BehavioSec, Innovatrics, FaceKey
Recruitment	Affective computing based on computer vision, voice and speech recognition and natural language processing (NLP)	AI-powered job interviews and personality assessments to evaluate candidates	Pymetrics, HireVue, Retorio
Monitoring	Affective computing based on voice recognition and NLP; wearable movement trackers; eye movement trackers; smart mouse	Worktime control, productivity and activity tracking, performance measurement	Cogito, WorkSmart, Geodis, Humanyze
Safety and wellbeing	Smart wearables; Computer vision	Accident prevention; physical and psychosocial health risk management	StrongArm Technologies, Fitbit, (many technologies in development)

Source: Bruegel.

We propose to classify biometric technologies according to their use by employers. We identify the following four groups of use (Table 1)[4]:

- Security: Security represents the classic use case for biometric technologies in workplaces. Allowing access to company resources to only authorised personnel is traditionally done using passwords, pin codes or key(card)s, but biometric authentication, such as face or

4 It should be noted that this classification is, to a certain extent, artificial: the boundaries between different uses of technologies are often blurred. So for example a technology used for security may also be used for monitoring. Nevertheless, we propose a classification which, in our view, best captures the differences between the applications that have been so far developed.

fingerprint recognition, offers benefits in terms of accuracy, security and efficiency.

- Recruitment: The purpose of AI systems in recruitment, including biometrics, is to create objective, data-driven candidate evaluations, for example through automated interviews or psychometric assessments.
- Monitoring: The digitalisation of work in many sectors has created new possibilities for uninterrupted and comprehensive worker surveillance. With biometric AI, employers can keep track of productivity, for example through keyboard logging or movement sensors, or measure performance using affective computing, concentration tracking or social metrics.
- Safety and wellbeing: One of the arguably most promising use cases for AI in workplaces is to improve worker health and safety. AI can help address a wide range of causes of morbidity by reducing the risk of accidents, burnout and musculoskeletal disorders. Most of the biometric systems we review rely on physiological data gathered through smart sensors and wearable devices that track muscle use, movement, fatigue or stress levels.

2.1 Security

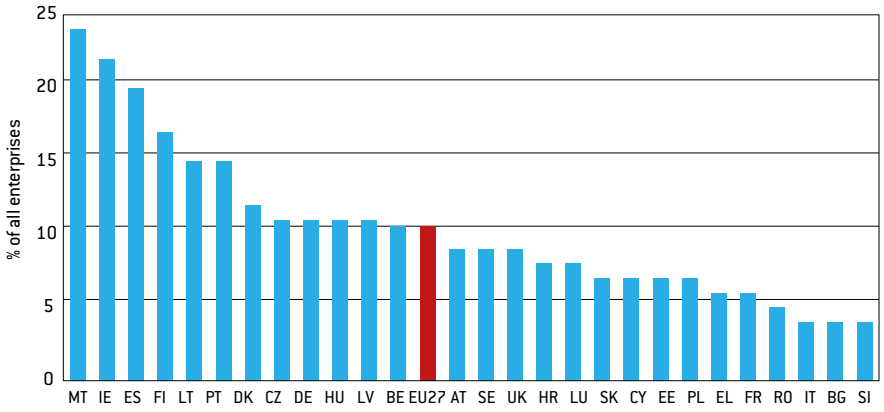
Table 2: Biometric AI for security

Employees		Employers	
Risk	Benefits	Risks	Benefits
Privacy issues, surveillance, function creep	Contactless identification, simplification, no risk of losing keycards/forgetting passwords	Data protection liability	Higher security, reduced risks of insider fraud

Source: Bruegel.

Security represents the classic use case for biometric technology in workplaces. Companies have an interest in restricting access to their facilities, data and resources to authorised personnel only, which necessitates a process of identity verification. Figure 2 shows the rate of use of biometric authentication methods in EU countries and in the United Kingdom, in 2019. One in ten of all EU companies rely on biometric authentication and verification in the workplace, with use rates ranging from as high as 24 percent in Malta to only 4 percent in Slovenia and Bulgaria. Fingerprint recognition is by far the most popular type of biometric authentication, followed by facial recognition, according to a survey of IT professionals[5].

Figure 2: Use of biometric authentication in enterprises, 2019



Source: Eurostat. Note: Data for the Netherlands is not available.

5 Peter Tsai, 'Data Snapshot: Biometrics in the Workplace Commonplace, but Are They Secure?', *Spiceworks*, 12 March 2018, available at https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure

There are several benefits to biometric authentication compared to conventional security systems. In contrast to knowledge-based (passwords, pin codes) or token-based (key cards) security systems, biometric authentication systems rely on characteristics inherent to someone's person. While passwords and key cards can be lost or stolen, biometric recognition guarantees that the individual in question is physically present. Biometric authentication is also more time- and cost-efficient, since the automated process only takes seconds, if that, and no human identity check is needed. Moreover, biometric features cannot be forgotten and therefore time-consuming recovery or reset processes needed for forgotten passwords or key cards are avoided. The passive nature of behavioural biometrics such as gait or keystroke recognition allows continuous authentication to ensure that the person accessing company data, accounts or other resources is indeed the one authorised to do so. For these reasons, behavioural biometrics are increasingly used for fraud detection and insider threat management (Hu *et al*, 2019; Liang *et al*, 2020). Therefore, enhancing conventional security systems with biometric identity recognition is to date the most secure, effective and efficient way to secure access to company property (Sabhanayagam *et al*, 2018)[6].

Privacy is at the core of concerns about the collection, storage and processing of biometric data

Reliance on employees' personal biometric characteristics for security has significant implications for workplaces and workers. Privacy is at the core of concerns about the collection, storage and processing of biometric data (Carpenter *et al*, 2018; Holland and Tham, 2020).

Beyond being a unique feature of a person, biometric data can contain a wide range of additional, personal information, which can potentially be extracted. For example, the continuous recording of keystrokes for authentication will also capture the content that is typed, including potentially sensitive personal information. Physical biometrics, such as fingerprints or hand geometry, may reveal private medical information. For example, Holland and Tham (2020) explained that fingerprints can be used to detect genetic disorders, and Carpenter *et al* (2018) argued that biometric samples allow the extraction of genetic markers that reveal potential health issues, such as hand swelling associated with sickle cell disease. The mere possibility of extraction of this information from biometric data opens up new questions about privacy, and could lead to discrimination between workers.

The use of workers' biometric data for undisclosed purposes without their knowledge and consent is a central concern (Carpenter *et al*, 2018; Holland and Tham, 2020). Beyond assessing medical risks, organisations could use the data to conduct background checks or, as is being done in the US, cross-reference biometrics with immigration records to identify undocumented immigrants (Goldstein and Alonso-Bejarano, 2017). Organisations could use the data to expand monitoring and surveillance, for instance by retracing employees' activities using historical authentication data. The GDPR prohibits function creep via the principles of data minimisation and purpose limitation. Employers that want to expand the use of biometric data beyond previously agreed functions would need to obtain renewed employee consent. Critics point to the challenges of enabling meaningful and informed consent for data collection in an employer-employee relationship[7].

Finally, there are concerns about potential data breaches and third-party access to personal (biometric) data. One of the key benefits of biometric systems, the fact that they rely on inherent characteristics rather than on knowledge or tokens, also implies that biometric features are irreplaceable: in case of a compromise, biometric ID cannot be changed like a password.

6 An additional potential benefit is the potential of touchless biometric security to limit infectious disease transmission: US-based IT firm Hewlett Packard Enterprise adopted a facial recognition access system to reduce COVID-19 infection risk compared to, for example, machines requiring PIN code entry. See: https://www.hpe.com/us/en/newsroom/press-release/2020/06/hpe-to-deliver-five-new-return-to-work-solutions-to-help-organizations-accelerate-recovery-in-wake-of-covid-19.html, accessed 6 August 2021.

7 For a discussion of the complexity of meaningful consent to data collection within the employer-employee relationship, see Moore (2020).

2.2 Recruitment

Table 3: Biometric AI for recruitment

Employees		Employers	
Risk	Benefits	Risks	Benefits
Discrimination, spurious correlations, bias, lack of feedback	Potentially more objective interview	Liability, loss of talent due to spurious correlations	Cost reduction, potentially more equality in the hiring process

Source: Bruegel.

Recruitment is an obvious application field for AI-driven analytics because hiring decisions are known to be riddled with human bias and discrimination (Bertrand and Mullainathan, 2004; Carlsson and Eriksson, 2019; Drydakis, 2009; Rooth, 2009; Tilcsik, 2011). Hence, many AI-powered recruitment tools are developed and adopted specifically with the aim of eliminating this problem from the selection process by offering an objective, data-driven and comparable assessment of candidates (Sánchez-Monedero *et al*, 2019). Virtually every Fortune 500 company is currently using some form of applicant-tracking system in their hiring processes[8]. However, to the best of our knowledge, representative, reliable data on the use of AI in recruitment, in particular interview systems or other biometrics, currently does not exist.

There is certainly potential for AI systems to enhance recruitment processes. Cowgill (2018) showed that AI can be better than a human counterfactual if certain conditions are met. He found that using a machine-learning algorithm to screen curriculum vitaes can do better than humans if the training data is sufficiently noisy. The algorithm was built on text mining and natural language processing assessing factors including education and work experience, as well as soft skills. The algorithm led to selection of candidates who were more likely to pass the interview process, accept job offers and be more productive once hired[9]. The algorithm was more likely to select candidates who graduated from non-elite colleges without job referrals or prior experience, but who had strong non-cognitive soft-skills.

Biometric data is primarily collected during the interview process or through personality assessments, in which candidates' behaviour – including their facial expressions, pitch and choice of words – feed into an AI-driven assessment of competences and personality[10]. In order to assess a candidate's suitability for a vacancy, interview systems are trained using data on the company's existing staff. Their test scores are combined with corporate performance benchmarks to identify correlations between the AI's analysis and job success. The AI then compares candidates' scores with those of the existing staff and groups applicants according to their probability of job success. Unilever, which relies on such an AI-enhanced recruitment tool for entry-level positions, claims the software has contributed to raising ethnic and socioeconomic diversity among new employees, in addition to saving 100,000 hours of interview time and $1 million in recruitment costs each year[11].

Drawing conclusions about emotional states or personality from video or tone recordings

8 Linda Qu, '99% of Fortune 500 Companies Use Applicant Tracking Systems', *Jobscan*, 7 November 2019, available at https://www.jobscan.co/blog/99-percent-fortune-500-ats/

9 The experiment was designed so that the algorithm's recommendation randomly overrode the choices of human recruiters about who to invite for interview. The effects measured were derived from candidates selected by the algorithm but not by the human recruiter.

10 Drew Harwell, 'A face-scanning algorithm increasingly decides whether you deserve the job', *Washington Post*, 6 November 2019, available at https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job

11 Minda Zetlin, 'AI Is Now Analyzing Candidates' Facial Expressions During Video Job Interviews', *Inc.*, 28 February 2018, available at https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html

without human intervention is however challenging and potentially problematic, in particular when the automated evaluation is the basis for hiring decisions.

A key question that needs answering even before considering its potential usefulness in the workplace is whether or not AI is capable of doing what it claims. A review of the literature by Barrett *et al* (2019) emphasised that technology companies overestimate the scientific validity of their base assumption that there is universal emotional expression. Instead, the authors found that emotional facial expression is highly context-specific, and that this variation is still understudied. They concluded that not only it is premature to use technology to draw conclusions about people's internal states, such analyses may completely lack validity if they fail to include the context of the individual (Barrett *et al*, 2019).

Furthermore, there is a major transparency issue (Raghavan *et al*, 2019; Sánchez-Monedero *et al*, 2019). It is currently not possible for researchers to evaluate the validity of the assessments. Developers of AI-powered hiring tools are reluctant to make their code or data available for independent audits, given their proprietary and sensitive natures. They furthermore rely on their own definitions of unbiased or fair algorithmic assessment, as currently there are no regulations in force that provide a legal standard for these terms. Given that the tool is trained on the set of current staff for each vacancy, characteristics of performance vary from job to job. Sánchez-Monedero *et al* (2019) concluded that even the most transparent providers fail to disclose how job-seekers can learn how their performance affected the system's evaluation. AI-backed systems are not geared to provide information on which factors (ie facial expression, voice, pitch) and parameters influence their assessments. In the case of the recruitment tools, this implies that neither candidates nor human resources managers can follow and retrace AI-based decision-making. The key risk, as a result, is spurious correlations. It is, for example, known that factors including lighting feature obstruction (such as covering part of the face with the hand), and expression intensity influence significantly the outcome and accuracy of computer-vision affective computing models (Patel *et al*, 2020).

Finally, one of the most important discussions around AI is the prevalence of bias. Rhue (2018) found that a vision-based sentiment-analysis AI assigned more negative feelings to black faces. Similarly, racial bias has been found in algorithms for natural language processing because of lack of knowledge and understanding of the cultural determinants of linguistic emotional expression (Sap *et al*, 2019). Furthermore, affective computing and recruitment AI tools are 'ableist' by default, by assigning certain features of speech, body language and facial expression paramount importance for job performance, though they have little to do with actual suitability and are unattainable for people with disabilities (Whittaker *et al*, 2019). While some technology companies claim to undertake efforts to counter such bias by continuously auditing their algorithms, decision-making processes continue to lack transparency and traceability. AI systems are known to frequently encode and perpetuate existing patterns of bias, and the rapid rollout of such tools without meaningful requirements or regulations imposed on them leads to the suspicion that they will exacerbate discrimination through their in-group and out-group classification systems (Crawford *et al*, 2019)

2.3 Monitoring

Table 4: Biometric AI for workplace monitoring

Employees		Employers	
Risk	Benefits	Risks	Benefits
Surveillance; loss of autonomy and control; mistrust between employee and employer, reduced job quality	Objective accounting of work efforts	Lower job quality could lead to higher employee turnover	Reduce time theft ('buddy-punching'); enhance productivity; improve performance

Source: Bruegel.

Interest in using technology to monitor and control what workers do is booming; COVID-19 and the shift to remote work have exacerbated this

Monitoring employees is not a new concept. Yet, in contrast to direct supervision by a physically present superior, the digitalisation of work and the internet of things (IoT) enables continuous and comprehensive tracking of all of workers' activities (Edwards *et al.*, 2018).

Interest in using technology to monitor and control what workers do is booming. The COVID-19 pandemic and the shift to remote work has exacerbated a trend already present before the crisis. In 2018, Gartner found that more than half of large corporations had adopted non-traditional monitoring techniques, up from 30 percent in 2015 (Kropp, 2019)[12]. During the pandemic, demand for biometric-monitoring AI soared, and one out of four companies introduced technologies to track their employees' behaviour passively (Kropp, 2021; Mascellino, 2020).

Workplace applications centre on tracking attendance, activity or performance. The most frequent technological methods of workplace surveillance tend to be monitoring of work emails, browser histories and files, CCTV and the recording and logging of phone calls (however, no granular data on use of monitoring technologies by EU companies is available). Monitoring via wearable devices is more common in workplaces that require a lot of physical activity, such as warehouses or construction sites.

Many workplaces re-apply biometric security devices for the purpose of worker monitoring. For example, fingerprint-based attendance tracking systems are widely commercially available. Advocates of the technology claim that such systems make attendance tracking more efficient while preventing some workers from clocking-in for others, improving productivity for both management and workers. However, these systems were ruled illegal in Germany in 2020, barring exceptional circumstances (Burt, 2020). Because the systems collect highly personal data, they run afoul of European GDPR laws.

When biometric data is combined with productivity-centred algorithms, the technology can be used to push efficiency and accuracy, potentially at the cost of surveillance and lower job quality (Gutelius and Theodore, 2019). Headlines about the deeply automated tracking processes in an Amazon warehouse offer an exemplary description of the risks of algorithmic monitoring and management. According to one report[13], workers wear a type of tracker that monitors their location and movements as well as their work activity. Based on historic data, an algorithm establishes standardised productivity rates and benchmarks to be attained by each employee. The tracking device also measures time-off-task and sends automatic alerts to workers if the period between measured work activities becomes too long. Reportedly, the AI system included an automated termination process: it would autonomously fire workers when quality or productivity benchmarks weren't maintained. Since thresholds were set to near-unattainable standards, workers were put under such significant time pressure that they would skip bathroom breaks in order to fulfil their artificially set benchmarks.

Discouraging and timing toilet breaks represents a questionable control over basic human needs and also raises issues around equality, illustrated by a number of reported instances in Europe where female employees (not of Amazon) were asked to wear specific clothing to signal when they were menstruating to receive permission to use the restrooms more often[14].

In office settings, a similarly comprehensive picture is painted by AI-driven sociometric devices: small, wearable badges capable of tracking individual and collective behaviours at work based on audio, movement, proximity and location data. In combination with

12 Gartner defines monitoring as *"analysing the text of emails and social-media messages, scrutinising who's meeting with whom, gathering biometric data and understanding how employees are utilising their workspace."*

13 Information in this paragraph is taken from Colin Lecher, 'How Amazon Automatically Tracks and Fires Warehouse Workers for "Productivity"', *The Verge*, 25 April 2019, available at https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

14 See for example Kate Connolly, 'German supermarket chain Lidl accused of snooping on staff', *The Guardian*, 27 March 2008, available at https://www.theguardian.com/world/2008/mar/27/germany.supermarkets, and Ian Sparks, 'Boss orders female staff to wear red bracelets when they are on their periods', *MailOnline*, 30 November 2010, available at https://www.dailymail.co.uk/news/article-1334400/Female-staff-Norway-ordered-wear-red-bracelets-period.html.

corporate metrics on output and performance, AI can link specific behaviours, such as talkativeness, or whether a worker dominates conversations, to productivity, identify (un-) productive processes and make suggestions to improve organisational efficiency (Eveleth, 2019; Ito-Masui *et al*, 2021). Although linking a badge to the wearer's identity requires consent according to the developers, critics argue that surveillance opportunities remain within reach, in particular in small or medium-sized entities (Moore, 2020).

Affective computing can also play a role in monitoring work performance. A US start-up called Cogito developed an AI system for call centres which assesses the mood of customers during phone calls and cues agents to adapt their way of speaking accordingly. Using voice analysis and natural language processing, the technology detects over 200 indicators of emotional state of both the customer and the agent in real-time. When it identifies a certain emotional state in a customer – for example frustration – it alerts the agent to speak more slowly, or display more empathy. Importantly, the AI serves not only as a tool to improve customer satisfaction, but also to monitor workers, as supervisors have "*the ability to proactively listen to live calls with no extra setup required* [and] *are automatically alerted to calls in which a customer is having a poor experience*"[15].

Automated monitoring may ensure that well-performing workers are identified and rewarded in a more consistent and objective manner. However, this comes at a cost of constant surveillance. The psychosocial risks associated with constant algorithmic monitoring are real and must be taken into account (Nurski, 2021).

2.4 Safety and wellbeing

Table 5: Biometric AI for health, safety and wellbeing

Employees		Employers	
Risk	Benefits	Risks	Benefits
Surveillance; collection of intimate health data; function creep; privacy	Prevention of accidents and adverse health outcomes	Liability for data protection	Reduction in incident costs

Source: Bruegel.

Workplaces can be dangerous. In 2018, 3332 workers in the EU died in an accident at work[16]. In addition, there were over three million serious non-fatal accidents in European workplaces[17]. In the EU, most workplace accidents occur in a handful of sectors. Agriculture, manufacturing, construction and transport account for over 65 percent of all fatal accidents. The most prevalent causes of workplace accidents in industrial settings are, in decreasing order of frequency, falls from heights, strikes by moving or falling objects, machine contact, ie when a worker is caught between parts of a machine, and being hit by moving vehicles (Svertoka *et al*, 2021).

Non-fatal illnesses also burden workers. Musculoskeletal disorders, together with cancer and circulatory illnesses, are the leading causes of work-related morbidity in the EU (Elsler *et al*, 2017). Workplace accidents, deaths and health problems generate massive costs that burden not only employers and employees but also public budgets and society as a whole. The European Agency for Safety and Health at Work (EU-OSHA) estimated that the costs of work-related accidents and illnesses in the EU amount to at least €476 billion per year, equal to about 3.3 percent of EU GDP (Elsler *et al*, 2017).

Technology may offer a solution to improve workplace safety. More and more smart technological solutions are available to address a wide range of work-related health issues. Instead of a reactive approach to accidents and health problems, these systems enable pre-

15 See https://cogitocorp.com/product/.

16 Eurostat hsw_n2_02.

17 Eurostat hsw_n2_01. Serious is defined as causing at least four days absence from work

ventive action by detecting hazards and risks before they manifest themselves in accidents or illnesses (Pavón *et al*, 2018). Through sensors, these systems gather data from the workers and their surroundings aimed at environmental sensing, proximity detection and location tracking (Awolusi *et al*, 2018; Svertoka *et al*, 2021). Biometric AI systems typically combine data collected on workers from physiolytic equipment, with environmental data gathered from other sensors or cameras (Svertoka *et al*, 2021). Physiolytics are wearable devices that use measurements of body functions, such as heart rate, muscle use or blood oxygen level, in machine-learning models and data analytics, from which AI draws conclusions about the physical and sometimes psychosocial state of the wearer (Mettler and Wulf, 2019). Wearables include fitness trackers, smart watches, patches and sensors attached to the body, smart clothing and personal protective equipment (PPE) (Svertoka *et al*, 2021).

Biometrics can help through five broad channels: (1) increasing compliance with PPE requirements and preventing falls; (2) addressing hazard caused by fatigue; (3) reducing sedentary behaviour and physical inactivity; (4) limiting psychosocial stress; (5) reducing physical stress and musculoskeletal disorders[18].

1. *Increasing compliance with PPE and preventing falls*. Records from the US Bureau of Labor show that in most incidents resulting in severe injury, workers were not correctly wearing PPE, suggesting that the severity of the incident could have been reduced with full PPE compliance (Kritzler *et al*, 2015). AI-driven solutions to PPE compliance are typically based on either computer vision or smart wearable technology. For example, a smart helmet can detect whether it is worn or not and determine the instant it is taken off using humidity sensors (Tan *et al*, 2021). In other instances (eg see Kritzler *et al*, 2015), workers may wear a smartwatch that signals which PPE is required for the task and recognises whether it is worn at that point in time. When a worker approaches a work station, the machinery and industrial equipment will only activate if she wears the right gear, as determined by the watch. Similarly, AI systems can help reduce the number of falls by identifying hazardous areas in workplaces using recordings of stumbling or loss of balance from smart sensors. Supervisors can use the data to detect hazardous locations on their worksites before an incident occurs, and address specific risks with targeted measures, without disrupting workers in their tasks.
2. *Addressing hazard caused by fatigue*. According to neuroscientific research, constant and long-term exposure to high-risk environments, such as construction sites, and the resulting familiarity with hazardous surroundings, lowers people's risk sensitivity and risk-judgement capabilities (Niv *et al*, 2012). A range of wireless, wearable sensing devices has been developed to measure and assess the level of attention or situational awareness of workers in real-time using physiological biometrics such as eye-movement or brain signals. Amazon, for example, deploys AI-powered cameras in its delivery vehicles to improve safety following a number of serious car accidents[19]. The vision system observes and records all drivers at all times and issues alerts for unsafe driving behaviour, such as speeding, fatigue or distracted driving. However, reports suggest that the technology sometimes unduly penalises drivers, negatively impacting their ability to earn income[20].
3. *Reducing sedentary behaviour and physical inactivity*. A number of health risks, including obesity, cardiovascular diseases and back pain, are associated with a lack of physical activity and extensive sedentary behaviour, typical of office environments. Workplace interventions to promote wellbeing and physical activity among employees often involve providing workers with wearable fitness trackers, such as FitBits, to monitor and track their

18 A detailed analysis of each of the five channels is reported in Hoffmann and Mariniello (2022).

19 See Tyler Sonnemaker, 'Amazon Is Deploying AI Cameras to Surveil Delivery Drivers "100% of the Time"', *Business Insider*, 3 February 2021, available at https://www.businessinsider.com/amazon-plans-ai-cameras-surveil-delivery-drivers-netradyne-2021-2.

20 See Sarah Jackson, 'Amazon's AI-powered cameras punish its delivery drivers when they look at side mirrors or when other cars cut them off, report says', *Business Insider*, 20 September 2021, available at https://www.businessinsider.com/amazon-delivery-drivers-netradyne-ai-cameras-punished-when-cut-off-2021-9

daily physical activities (Glance *et al*, 2016; Nikayin *et al*, 2014). Large-scale collection and analysis of workers' data can provide the basis for specific health interventions to address emerging risks early on. However, whether this justifies constant monitoring of physical activity, in particular outside of working hours, should be judged by each individual worker.

4. *Limiting psychosocial stress*. A study by the World Health Organisation and International Labour Organisation identified a direct relationship between overwork and premature death (Pega *et al*, 2021)[21]. Lasting psychosocial stress at work increases the risk of illness and death from heart disease and stroke. Moreover, chronic stress can lead to negative mental health outcomes. It is, for instance, a crucial cause of burnout (Salvagioni *et al*, 2017). More than half of the European labour force reports commonly experiencing work-related stressors in their jobs (EU-OSHA, 2013). Recent technological advances in biometric technology have enabled the direct measurement of stress in the workplace. The benefits are straightforward: early identification of chronic stress and its underlying causes can enable targeted, effective and timely preventive action by employers to mitigate the risk of adverse health outcomes in their organisations.
5. *Reducing physical stress and musculoskeletal disorders.* Physical stress can lead to musculoskeletal disorders (MSDs), one of the leading causes of occupational morbidity. Processes and environments in certain workplaces, like construction sites, assembly lines and warehouses, pose several risk factors for MSDs, including repetitive motions, force and awkward postures (Nath *et al*, 2017). However, ergonomic risks also emerge from tasks and occupations that do not require heavy labour but entail very repetitive motions, for example typing on a keyboard (Valero *et al*, 2016) or scanning products at a supermarket check-out (Peppoloni *et al*, 2016). Biometric or biomechanical measurement tools, usually consisting or sensors worn on the worker's body, directly and accurately measure individual body movements over time and allow the identification of unsafe movements and detection of hazardous kinetic patterns (Nath *et al*, 2017; Valero *et al*, 2016).

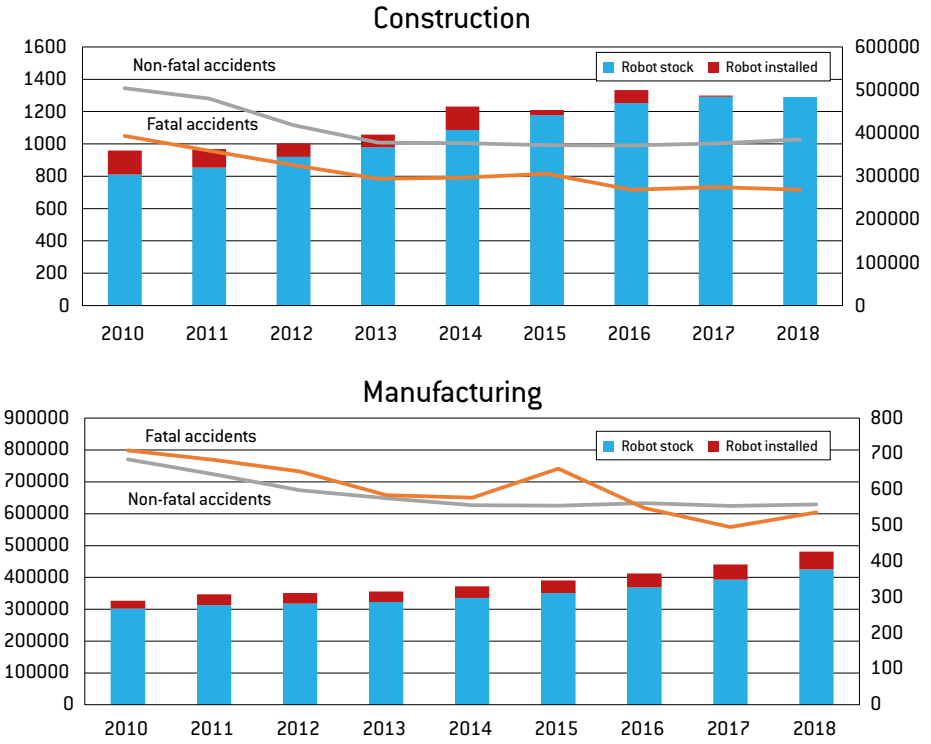
Biometric technology used for safety purposes appears to have the greatest potential to benefit workers and employers alike. Nonetheless, its use is not risk-free. Workers may be concerned about their behaviour being constantly monitored. Workers' safety data may be accessed by their employers to assess their performance, undermining the primary goal of the adopted technology. Physical and mental health information should not be used as a workforce management tool. Mood-recognition AI trained to associate biophysical states with stress levels and mood can allow employers to "*use this information to understand the general feeling of the work environment at any given time without explicitly asking any employees*" (Zenonos *et al*, 2016), which would to many appear to be a strong encroachment on privacy, in particular since changes in mood are not necessarily related to work. In addition to implications for data security, access by third-parties and function creep, the potential use of stress and mood-detection AI in workplaces raises the question of whether employers should come to know these things when their staff choose not to communicate them.

21 Measured effect of 55+ working hours per week compared to regular (35-40) working hours.

Box 1: Computers are everywhere except in workplace safety statistics

Biometric technologies have a great potential to increase safety at work. However, in sectors in which adoption of digital technologies has constantly increased in the past years, there has been no corresponding drop in injury rates. Statistical information on the use of AI-powered biometric equipment in the EU is not yet available, but we can use proxies: it is reasonable to assume that sectors in which digitisation and robotisation are higher also tend to have a higher rate of adoption of biometric technologies. Figure 3 compares the trend of robot adoption with workplace accidents in Europe. It might be expected that, as production processes become more automated, injuries would also become less frequent. However, that is not observed in the data: most of the growth in adoption of robotics took place after 2013/2014, but injury rates declined mostly before that. While the insights from this analysis cannot be conclusive because of the lack of detailed data on the type of technology adopted by companies, they nevertheless suggest that worker safety does not seem yet a significant driver of companies' technological investment.

Figure 3: Workplace accidents and robotics adoption in industry, EU28



Source: Eurostat and World Robotics. Note: number of fatal accidents in manufacturing and number of non-fatal accidents in construction expressed on the right axis.

3 From theory to practice to policy

The taxonomy of biometric technologies used in the workplace that we have described above has one primary purpose: to help make more concrete what the European Commission has only sketched in broad terms in its AI Act proposal. The Commission is right to emphasise that using AI in the workplace can be very risky. But grasping the dynamics through which technology and actual harm are linked is an essential condition for effective regulation.

We note that there is a significant scarcity of data at granular level. This scarcity prevents observers from monitoring the implications of the adoption by employers of new technologies. While progress is being made in terms of data collection on technological adoption by European companies (for example, Eurostat has now indicators that monitor uptake of AI technology), statistics still lack detail on the type of biometric technology used. The AI Act may help partially to address that issue, in that it imposes notification obligations to providers of high-risk applications. The European Commission plans to establish a system for registering standalone high-risk AI applications in a public EU-wide database, and this is a welcome development. Yet, the database will be mostly driven by the information supplied by the AI application providers, which may not be able to accurately foresee all potential risks that can emerge at user level. It would be preferable to design coherent statistical systems for capturing information directly from EU employers about AI use.

The AI Act should also broaden the scope of what it considers 'biometric data': it currently relies on the definition adopted in the GDPR, which hinges on the application of the information collected to identify individuals. However, as we have discussed, biometric technologies may have detrimental effects on workers even if not strictly used for personal identification (for example, data can be lawfully collected at personal level, but raw aggregate biometric data can be stored and used to control the workforce collectively).

For individual workers, biometric technologies pose a variety of risks; these are pervasive and represent a significant barrier

For individual workers, biometric technologies in the workplace pose a variety of risks. There are privacy concerns: devices collect a myriad of detailed, sensitive data, with the risk that these may be accessed by (unauthorised) third parties or used by the employer without the employee's consent for purposes other than initially foreseen. These risks are pervasive and represent a significant barrier. There is a potential loss of personal freedom or control over how employees organise their work. Knowing their employer has constant access to real-time metrics on their effort level can induce workers to change their behaviour and eventually leave them with less motivation and engagement. There is a risk of overreliance on the technology. This is particularly problematic when a technology's accuracy is overestimated. Not only can this leave workers unorganised in the case of a technology outage, it can also cause them to trust the device's recommendations more than their own feeling of wellbeing at the time. From the perspective of workers, this also raises the question of whether it can be assumed that employers are capable of interpreting the output from AI correctly, or if they take the results as truth, though results are potentially biased.

Nevertheless, some technologies have huge potential to address long-standing issues. This in particular refers to safety and security in the workplace which is a major, often underrated, problem in European labour markets. It is thus important to ensure that any new regulatory requirement does not dissuade employers from adopting technologies that have a high potential to protect workers from injury or other health hazards. Based on our taxonomy, it should be possible to design systems of incentives for providers to deploy innovative solution that maximise benefits while complying with the risk-mitigation rules, having in mind the final effect on workers. Likewise, users could be steered to invest more in technologies that can help address workers' issues, rather than exacerbate them. For example, any discussion related to taxation of digital technologies (Christie, 2021) should be informed by that trade-off: 'robot taxes' do not necessarily need to focus on the quantity of jobs potentially destroyed by technology. Rather they could be informed by the balance of risks and benefits which we have described in this paper. For example, it would be desirable to craft a taxation system

that would reward employers that adopt technologies with high potential to increase safety at work while, if anything, penalising use of technology that can harm workers through intensive monitoring or automated emotional scrutiny. The European Commission in June 2021 issued the 'Strategic Framework on Health and Safety at Work 2021-2027', which outlines actions to improve workers' health and safety in a changing world of work (European Commission, 2021b). In this strategy, the Commission also recognises the potential of new technologies, including artificial intelligence, to improve occupational health, safety and wellbeing.

On a broader level, our analysis clearly indicates that no biometric technology can be considered intrinsically bad or good for workers. In other words, working hard to ensure that technology delivers accurate results, and that artificial intelligence systems are not conditioned by bias at any level of the value chain (development, data sourcing, distribution and use), do not guarantee no harm. Addressing bias is a necessary but not sufficient step to protect humans from harm. Unbiased biometric monitoring of workers may deliver fairer assessments of worker performance, but it can still entail a worsening of their wellbeing, increasing their stress levels, for example. That conclusion emphasises the role of risk management at local level by users of high-risk AI applications. Employers should not mindlessly adopt biometric technologies in their facilities or offices. Nor can they rely on providers' reassurances about the potential risks of the applications they develop (as it is currently suggested by the proposed AI Act). Employers of significant size should rather be required to evaluate the impact of the implementation of high-risk technologies before adoption, possibly though the active involvement of their workforce. After adoption, employers should survey their workers' feelings and assess the effects on their wellbeing.

References

Awolusi, I., E. Marks and M. Hallowell (2018) 'Wearable Technology for Personalized Construction Safety Monitoring and Trending: Review of Applicable Devices', *Automation in Construction* 85: 96–106

Balan, O., G. Moise, L. Petrescu, A. Moldoveanu, M. Leordeanu and F. Moldoveanu (2020) 'Emotion Classification Based on Biophysical Signals and Machine Learning Techniques', *Symmetry* 12(1): 21

Barrett, L.F., R. Adolphs, S. Marsella, A.M. Martinez and S.D. Pollak (2019) 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements', *Psychological Science in the Public Interest* 20(1): 1–68

Bertrand, M. and S. Mullainathan (2004) 'Are Emily and Greg More Employable Than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination', *American Economic Review* 94(4): 991–1013

Burt, C. (2020) 'Biometric Time and Attendance Systems Restricted by European Data Protection Rules, Dutch Authority Issues Fine', *Biometric Update*, 4 May, available at https://www.biometricupdate.com/202005/biometric-time-and-attendance-systems-restricted-by-european-data-protection-rules-dutch-authority-issues-fine

Carlsson, M. and S. Eriksson (2019) 'Age Discrimination in Hiring Decisions: Evidence from a Field Experiment in the Labor Market', Labour Economics, Special Issue on European Association of *Labour Economists*, 30th Annual Conference, Lyon, France, 13-15 September 2018, 59: 173–83

Carpenter, D., A. McLeod, C. Hicks and M. Maasberg (2018) 'Privacy and Biometrics: An Empirical Examination of Employee Concerns', *Information Systems Frontiers* 20(1): 91–110

Christie, R. (2021) 'Do robots dream of paying taxes?' *Policy Contribution* 20/2021, Bruegel

Cowgill, B. (2018) 'Bias and Productivity in Humans and Algorithms: Theory and Evidence from Resume Screening', Columbia Business School, Columbia University 29

Crawford, K., R. Dobbe, T. Dryer, G. Fried, B. Green, E. Kaziunas ... M. Whittaker (2019) *AI Now 2019 Report*, AI Now Institute

Drydakis, N. (2009) 'Sexual Orientation Discrimination in the Labour Market', *Labour Economics* 16(4): 364–72

Edwards, L., L. Martin, and T. Henderson (2018) 'Employee Surveillance: The Road to Surveillance is Paved with Good Intentions', mimeo, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234382

Elsler, D., J. Takala, and J. Remes (2017) *An International Comparison of the Cost of Work-Related Accidents and Illnesses*, European Agency for Safety and Health at Work.

EU-OSHA (2013) 'European Opinion Poll on Occupational Safety and Health 2013', European Agency for Safety and Health at Work, available at https://osha.europa.eu/en/facts-and-figures/european-opinion-polls-safety-and-health-work/european-opinion-poll-occupational-safety-and-health-2013

European Commission (2021a) 'Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts', COM(2021) 206

European Commission (2021b) 'EU Strategic Framework on Health and Safety at Work 2021-2027 Occupational Safety and Health in a Changing World of Work', COM(2021) 323

European Commission (2020) *European Enterprise Survey on the Use of Technologies Based on Artificial Intelligence: Final Report*, available at https://data.europa.eu/doi/10.2759/759368

Eveleth, R. (2019) 'Your Employer May Be Spying on You – and Wasting Its Time', *Scientific American*, 16 August, available at https://www.scientificamerican.com/article/your-employer-may-be-spying-on-you-and-wasting-its-time/

Glance, D.G., E. Ooi, Y. Berman, C.F. Glance and H.R. Barrett (2016) 'Impact of a Digital Activity Tracker-Based Workplace Activity Program on Health and Wellbeing', DH'16: *Proceedings of the 6th International Conference on Digital Health Conference*

Goldstein, D.M. and C. Alonso-Bejarano (2017) 'E-Terrify: Securitized Immigration and Biometric Surveillance in the Workplace', *Human Organization* 76(1): 1–14

Gutelius, B. and N. Theodore (2019) *The Future of Warehouse Work: Technological Change in the U.S. Logistics Industry*, UC Berkeley Center for Labor Research and Education and Working Partnerships USA

Han, L., Q. Zhang, X. Chen, Q. Zhan, T. Yang and Z. Zhao (2017) 'Detecting Work-Related Stress with a Wearable Device', *Computers in Industry* 90: 42–9

Hoffmann, M. and M. Mariniello (2022) 'Artificial intelligence in the workplace: tackling the biometrics challenge', *Working Paper*, Bruegel, forthcoming

Holland, P. and T.L. Tham (2020) 'Workplace Biometrics: Protecting Employee Privacy One Fingerprint at a Time', *Economic and Industrial Democracy*, April

Hu, T., W. Niu, X. Zhang, X. Liu, J. Lu and Y. Liu (2019) 'An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning', *Security and Communication Networks*, vol. 2019, Article ID 3898951

Ito-Masui, A., E. Kawamoto, R. Esumi, H. Imai, and M. Shimaoka (2021) 'Sociometric Wearable Devices for Studying Human Behavior in Corporate and Healthcare Workplaces', *BioTechniques* 71(1): 392–9

Khowaja, S.A., A.G. Prabono, F. Setiawan, B.N. Yahya and S.-L. Lee (2021) 'Toward Soft Real-Time Stress Detection Using Wrist-Worn Devices for Human Workspaces', *Soft Computing* 25(4): 2793–820

Kritzler, M., M. Bäckman, A. Tenfält, and F. Michahelles (2015) 'Wearable Technology as a Solution for Workplace Safety', *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia*

Kropp, B. (2019) 'The Future of Employee Monitoring', Gartner, 3 May, available at https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring

Kropp, B. (2021) '9 Work Trends That HR Leaders Can't Afford to Ignore in 2021', Gartner, 6 April, available at https://www.gartner.com/smarterwithgartner/9-work-trends-that-hr-leaders-cant-ignore-in-2021

Liang, Y., S. Samtani, B. Guo, and Z. Yu (2020) 'Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective', *IEEE Internet of Things Journal* 7(9): 9128–43

Mascellino, A. (2020) 'Union Warns against Biometric Monitoring of Employees amid Increase in Remote Work', Biometric Update, 30 October, available at https://www.biometricupdate.com/202010/union-warns-against-biometric-monitoring-of-employees-amid-increase-in-remote-work

McStay, A. (2020) 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy', *Big Data & Society* 7(1)

Mehta, Y., N. Majumder, A. Gelbukh and E. Cambria (2020) 'Recent Trends in Deep Learning Based Personality Detection', *Artificial Intelligence Review* 53(4): 2313–39

Mettler, T. and J. Wulf (2019) 'Physiolytics at the Workplace: Affordances and Constraints of Wearables Use from an Employee's Perspective', *Information Systems Journal* 29(1): 245–73

Moore, P. (2020) *Data Subjects, Digital Surveillance, AI and the Future of Work*, Panel for the Future of Science and Technology, European Parliamentary Research Service

Nath, N.D., R. Akhavian and A.H. Behzadan (2017) 'Ergonomic Analysis of Construction Worker's Body Postures Using Wearable Mobile Sensors', *Applied Ergonomics* 62: 107–17

Nikayin, F., M. Heikkilä, M. de Reuver and S. Solaimani (2014) 'Workplace Primary Prevention Programmes Enabled by Information and Communication Technology', *Technological Forecasting and Social Change* 89: 326–32

Niv, Y., J.A. Edlund, P. Dayan and J.P. O'Doherty (2012) 'Neural Prediction Errors Reveal a Risk-Sensitive Reinforcement-Learning Process in the Human Brain', *Journal of Neuroscience* 32(2): 551–62

Nurski, L. (2021) 'Algorithmic Management Is the Past, Not the Future of Work', *Bruegel Blog*, 6 May, available at https://www.bruegel.org/2021/05/algorithmic-management-is-the-past-not-the-future-of-work/

Patel, K., D. Mehta, C. Mistry, R. Gupta, S. Tanwar, N. Kumar and M. Alazab (2020) 'Facial Sentiment Analysis Using AI Techniques: State-of-the-Art, Taxonomies, and Challenges', *IEEE Access* 8: 90495–519

Pavón, I., L.F. Sigcha, P. Arezes, N. Costa, G. Arcasand J.M. Lopez Navarro (2018) 'Wearable Technology for Occupational Risk Assessment: Potential Avenues for Applications', in P.M. Arezes, J.S. Baptista, M.P. Barroso, P. Carneiro, P. Cordeiro, N. Costa, R.B. Melo, A.S. Miguel and G. Perestrelo (eds) *Occupational Safety and Hygiene* VI, CRC Press

Pega, F., B. Náfrádi, N.C. Momen, Y. Ujita, K.N. Streicher, A.M. Prüss-Üstün ... T.J. Woodruff (2021) 'Global, Regional, and National Burdens of Ischemic Heart Disease and Stroke Attributable to Exposure to Long Working Hours for 194 Countries, 2000–2016: A Systematic Analysis from the WHO/ILO Joint Estimates of the Work-Related Burden of Disease and Injury', *Environment International* 154: 106595

Peppoloni, L., A. Filippeschi, E. Ruffaldi and C.A. Avizzano (2016) 'A Novel Wearable System for the Online Assessment of Risk for Biomechanical Load in Repetitive Efforts', *International Journal of Industrial Ergonomics, New Approaches and Interventions to Prevent Work Related Musculoskeletal Disorders* 52: 1–11

Raghavan, M., S. Barocas, J. Kleinberg, and K. Levy (2019) 'Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices', ACM Conference on Fairness, Accountability, and Transparency, 2020

Richardson, S. (2020) 'Affective Computing in the Modern Workplace', *Business Information* Review 37(2): 78–85

Rooth, D.-O. (2009) 'Obesity, Attractiveness, and Differential Treatment in Hiring A Field Experiment', *Journal of Human Resources* 44(3): 710–35

Sabhanayagam, T., V.P. Venkatesan and K. Senthamaraikannan (2018) 'A Comprehensive Survey on Various Biometric Systems', *International Journal of Applied Engineering Research* 13(5): 2276–97

Salvagioni, D.A.J., F.N. Melanda, A.E. Mesas, A.D. González, F.L. Gabani and S.M. de Andrade (2017) 'Physical, Psychological and Occupational Consequences of Job Burnout: A Systematic Review of Prospective Studies', *PLoS ONE* 12(10): e0185781

Sánchez-Monedero, J., L. Dencik, and L. Edwards (2019) 'What Does It Mean to 'Solve' the Problem of Discrimination in Hiring?' *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, January 2020

Sap, M., D. Card, S. Gabriel, Y. Choi, and N.A. Smith (2019) 'The Risk of Racial Bias in Hate Speech Detection', *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics. Association for Computational Linguistics*

Sundararajan, K. and D.L. Woodard (2018) 'Deep Learning for Biometrics: A Survey', *ACM Computing Surveys* 51(3): 65:1-65:34

Svertoka, E., S. Saafi, A. Rusu-Casandra, R. Burget, I. Marghescu, J. Hosek and A. Ometov (2021) 'Wearables for Industrial Work Safety: A Survey', *Sensors* 21(11): 3844

Tan, Y.H., A. Hitesh and K.H.H. Li (2021) 'Application of Machine Learning Algorithm on MEMS-Based Sensors for Determination of Helmet Wearing for Workplace Safety', *Micromachines* 12(4): 449

Tilcsik, A. (2011) 'Pride and Prejudice: Employment Discrimination against Openly Gay Men in the United States', *American Journal of Sociology* 117(2): 586–626

Valero, E., A. Sivanathan, F. Bosché and M. Abdel-Wahab (2016) 'Musculoskeletal Disorders in Construction: A Review and a Novel System for Activity Tracking with Body Area Network', *Applied Ergonomics* 54: 120–30

Vinciarelli, A. and G. Mohammadi (2014) 'A Survey of Personality Computing', *IEEE Transactions on Affective Computing* 5(3): 273–91

Whittaker, M., M. Alper, C.L. Bennett, S. Hendren, L. Kaziunas, M. Mills … S. Myers West (2019) *Disability, Bias, and AI*, AI Now Institute

Yanushkevich, S., S. Eastwood, K. Lai, and V. Shmerko (2020) 'Emerging Biometrics: Deep Inference and Other Computational Intelligence', *ArXiv*: 2006.11971

Zenonos, A., A. Khan, G. Kalogridis, S. Vatsikas, T. Lewis and M. Sooriyabandara (2016) 'HealthyOffice: Mood Recognition at Work Using Smartphones and Wearable Sensors', *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*