(mia.
ho mann@bruegel.org)
is a Research Assistant at
Bruegel

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

is Policy Contribution
was produced within the
project ‘Future of Work and
Inclusive Growth in Europe’,
with the nancial support
of the Mastercard Center for
Inclusive Growth

bru

1

Traditionally, the analysis of the impact of technology on labour markets has focused on

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 signi cant potential to a ect workers' well-being, a rst 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 classi ed 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 rms, 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 signi cant adoption barriers. ese barriers are not considered very problematic for other technologies.

e increasing interest of regulatory authority in these markets is therefore not coincidental. e European Union, for example, has been increasingly active in recent years in attempting to de ne a legal framework to mitigate the risks of abuse arising from advanced technology. e 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 arti cial intelligence, commonly referred to as the 'AI Act' proposal (European Commission, 2021a). e 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 speci cally lists as high-risk:

•

ngerprint recognition, o ers bene ts in terms of accuracy, security and e ciency.

- Recruitment: e 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: e 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 a ective 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

2

Employees		Employers	
Risk	Bene ts	Risks	Bene ts
Privacy issues, surveillance, function creep	Contactless identi cation, simpli cation, 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 veri cation. 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 veri cation 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].

2 , 201

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

Spiceworks, 0

2.2

3

Employees		Employers	
Risk	Bene ts	Risks	Bene ts
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 obvi1 talen

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 , (2019) emphasised that technology companies overestimate the scienti c validity of their base assumption that there is universal emotional expression. Instead, the authors found that emotional facial expression is highly context-speci c, and that this variation is still understudied. ey 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 , 2019).

Furthermore, there is a major transparency issue (Raghavan , 2019; Sánchez-Monedero , 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. ey furthermore rely on their own de nitions 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 sta for each vacancy, characteristics of performance vary from job to job. Sánchez-Monedero , (2019) concluded that even the most transparent providers fail to disclose how job-seekers can learn how their performance a ected the system's evaluation. AI-backed systems are not geared to provide information on which factors (ie facial expression, voice, pitch) and parameters in uence 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. e key risk, as a result, is spurious corre-

tus corchomerurrce AIy isplee(ib)1 (ib)1 v(ion-m)7.7ecte(e n)7 (o (ple)15s corc(s inm(de or d)15(P)2andid)
luus cor
ce

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 ., 2018).

Interest in using technology to monitor and control what workers do is booming. e

corporate metrics on output and performance, AI can link speci c behaviours, such as talkativeness, or whether a worker dominates conversations, to productivity, identify (un-) productive processes and make suggestions to improve organisational e ciency (Eveleth, 2019; Ito-Masui ., 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).

A ective 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 identi es 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 "[and] [15].

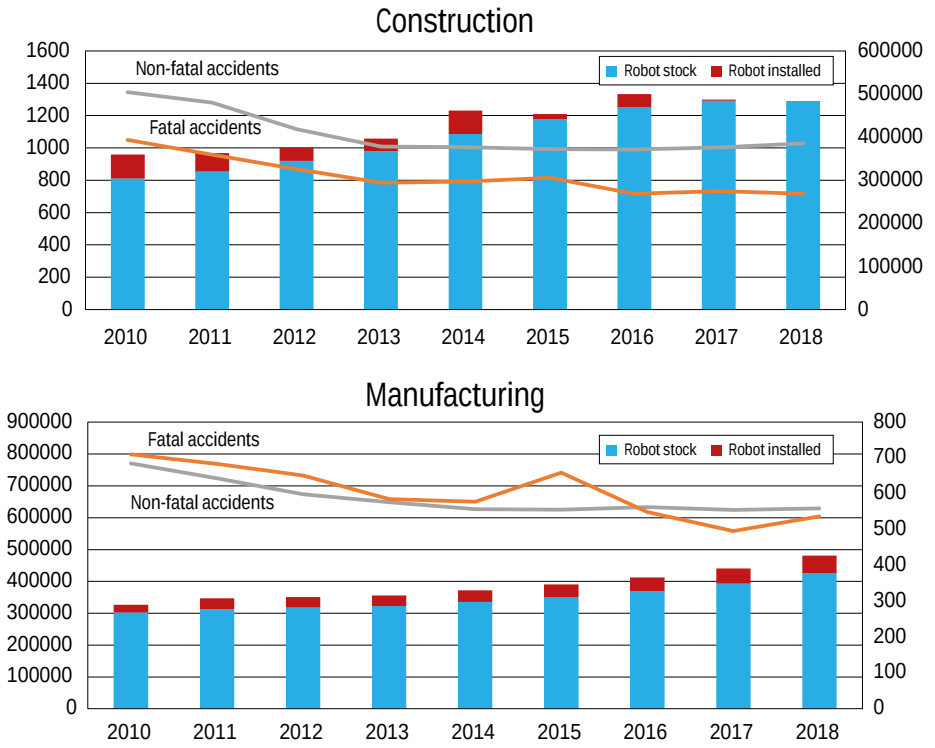
Automated monitoring may ensure that well-performing workers are identi ed and rewarded in a more consistent and objective manner. However, this comes at a cost of con-

ventive action by detecting hazards and risks before they manifest themselves in accidents or illnesses (Pavón ., 2018). rough sensors, these systems gather data from the workers and their surroundings aimed at environmental sensing, proximity detection and location tracking (Awolusi ., 2018; Svertoka ., 2021). Biometric AI systems typically combine data collected on workers from physiolytic equipment, with environmental data gathered from other sensors or cameras (Svertoka ., 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). Weara-

1

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 signi cant driver of companies' technological investment.

3 28



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

e 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. e 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 e ective regulation.

We note that there is a signi cant scarcity of data at granular level. is 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. e AI Act may help partially to address that issue, in that it imposes noti cation obligations to providers of high-risk applications. e 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.

e AI Act should also broaden the scope of what it considers 'biometric data': it currently relies on the de nition 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 e ects on workers even if not strictly used for personal identi cation (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 in the workplace pose a variety of risks. ere 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. ese risks are pervasive and represent a signi cant barrier. ere is a potential loss of personal freedom or control

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. e 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 arti cial intelligence, to improve occupational health, safety and wellbeing.

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

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

Edwards, L., L. Martin, and T. Henderson (2018) 'Employee Surveillance: e 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) *A* *C* *C* *A* , 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-_gures/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 Arti cial Intelligence (Arti cial 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) *B* *A* , available at https://data.europa.eu/doi/10.2759/759368

Eveleth, R. (2019) 'Your Employer May Be Spying on You – and Wasting Its Time,' *A* , 16 August, available at https://www.scienti_camerican.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: *6* , *C* *D* , *C*

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

Gutelius, B. and N. eodore (2019) *C* , 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,' *C* , 90: 42–9

Ho mann, M. and M. Mariniello (2022) 'Arti cial intelligence in the workplace: tackling the biometrics challenge', , Bruegel, forthcoming

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

Hu, T., W. Niu, X. Zhang, X. Liu, J. Lu and Y. Liu (2019) 'An Insider reat Detection Approach Based on Mouse Dynamics and Deep Learning,'

Rooth, D.-O. (2009) 'Obesity, Attractiveness, and Di erential Treatment in Hiring A Field Experiment', 44(3): 710–35

Sabhanayagam, T., V.P. Venkatesan and K. Senthamaraikannan (2018) 'A Comprehensive Survey on Various Biometric Systems', 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', 12(10): e0185781

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

Sap, M., D. Card, S. Gabriel, Y. Choi, and N.A. Smith (2019) ' e Risk of Racial Bias in Hate Speech Detection', *57*,

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

Svertoka, E., S. Saa , A. Rusu-Casandra, R. Burget, I. Marghescu, J. Hosek and A. Ometov (2021) 'Wearables for Industrial Work Safety: A Survey', 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', 12(4): 449

Tilcsik, A. (2011) 'Pride and Prejudice: Employment Discrimination against Openly Gay Men in the United States', 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', 54: 120–30

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

Whittaker, M., M. Alper, C.L. Bennett, S. Hendren, L. Kaziunas, M. Mills ... S. Myers West (2019) *D* , *B* , , AI Now Institute

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

Zenonos, A., A. Khan, G. Kalogridis, S. Vatsikas, T. Lewis and M. Sooriyabandara (2016) 'HealthyO ce: Mood Recognition at Work Using Smartphones and Wearable Sensors', *2016* *C* *C* *C* *C* *C* *C*